

# أمن المعلومات والمواقع وأجهزة الكمبيوتر والدفع الإلكتروني



كيف نؤمن بفساد أولادك من الهاكرز والاكراكرز  
كيف لنا ان نؤمن من الفيروسات



خالد محمد خالد

KHALED MOHAMED KHALED  
Internet specialist diploma

بسم الله الرحمن الرحيم  
نرفع درجات من ثناء وفوق كل ذي علم عليم  
صدق الله العظيم  
إعداد  
خالد محمد خالد

بكالوريوس العلوم - جامعة الإسكندرية  
وبلدم الدراسات العليا في الإنترنت  
من الولايات المتحدة الأمريكية

Khaled Mohamed Khaled

Internet and ecommerce specialist Diploma

Washington D.C., USA



المركز العلمي لتبسيط العلوم

١٢ حسن رفعت، سيدى بشر، إسكندرية، مصر

تليفون: ٥٢٩٨٤٢٨ - فاكس: ٥٢٩٨٤٢٨

بسم الله الرحمن الرحيم

(قَسْرٌ يَعْمَلُ مِثْقَالَ ذَرَّةٍ خَيْرًا يَرَهُ ،

وَمَنْ يَعْمَلْ مِثْقَالَ ذَرَّةٍ شَرًّا يَرَهُ )

صدق الله العظيم

إعلم أعي العزير ان ديننا أكنيفه حذر بعدم الإضرار بالناس إن كان في أرزاقهم او في علمهم او في انشطتهم ولا تكن من ذوى النفوس الضعيفت فهم جاهلون بان الله هو الرقيب وإنه سبحانه وتعالى ليس بظلام للعبيد .

فيمكنك ان تكون هاكم بل وكرام ولكن في سبيل الله ، ما بالك إذا إستخدمت كل ما لديك من علم و فنون وتقنيت في غلق المواقع الإباحية وتتبع أسرار العدو ، اليس ذلك في سبيل الله .

قال تعالى : " واما تخافن من قوم غيانت فانبد إليهم على سواء إن الله لا

يحب الكائنين " سورة الأنفال الآية ٥٨

### تذير :

حقوق الطبع والنشر لهذا الكتاب محفوظة للمركز العلمي لتبسيط العلوم ولا يجوز نشر أى جزء من هذا الكتاب أو إختزان أى جزء من مادته بطريقة الإسترجاع أو نقله بأى طريقة من الطرق الإلكترونية أو الميكانيكية أو بالتصوير أو التسجيل أو النسخ أو النقل دون الرجوع إلى المؤلف وأخذ تصريح خطى بذلك  
فصوف يعرض نفسه للمسائلة القانونية ،  
مع حفظ كافة حقوقنا الجنائية والمدنية ...

موسوعة التجارة الإلكترونية ( ١٢ )

أمن المعلومات

Information Security

رقم الإيداع بحار الكتب : ٢٠٠٦/٢١٤٠٢

ISBN: 977-6197-28-0

## رجاء

رحمت الله والذى ... قال لى ذات يوم  
لكل شيء زكاة وزكاة العلم تبليغه للآخرين ..  
اللهم إن كان هذا الكتاب فيه منفعة للامة العربية فاجعله  
فى ميزان حسنات والذى .. وبهذا العمل ادعو الله سبحانه وتعالى  
ان ينصر المسلمين فى كل بقاع الارض  
وان يخلص الاقصى المبارك من ايدي اليهود ...

## شكر وتقدير

جزى الله خيرا كل من ساعدنى فى اتمام هذا العمل المتواضع ليضع نور الاصل  
واخل عيدى واخذلتى واخذلتى مستخدمى شبكة الانترنت ....

## صدر من موسوعة التجارة الإلكترونية حتى الآن

١. البيع والشراء عبر مواقع المزادات داخل شبكة الإنترنت eBay
٢. كيف تصمم موقع يبيع منتجاتك عبر شبكة الإنترنت Web marketing
٣. التصدير والإستيراد باستخدام شبكة الإنترنت
- Import& Export through the Internet
٤. التسويق عبر البريد الإلكتروني e-marketing
٥. كيف تبسيع منات المنتجات الإسلامية عبر شبكة الإنترنت
٦. استخدام الـ drop shipping لعمل أرباح كبيرة بدون رأس مال
٧. التسويق باستخدام آلات البحث والدلائل
- 500 search engines and directories
٨. التسويق باستخدام البرامج المشاركة Affiliate programs
٩. نظم الدفع الإلكتروني Payment method
١٠. تعليم اللغة الإنجليزية التجارية للعمل بها عبر شبكة الإنترنت
١١. خدمة العملاء - استخدام الرسائل القصيرة والمنتديات والقوائم البريدية والشات.
١٢. أمن المعلومات

لمعرفة محتويات كل كتاب وكتب المؤلف (الأخرى)

الرجاء زيارة موقعنا على (الإنترنت)

<http://www.books4internet.com>

[scss@books4internet.com](mailto:scss@books4internet.com)

## تمهيد

لقد اعتمدت اعتماداً كلياً في كتابة هذا الكتاب على خبرتي المكتسبة في مجال العمل عبر شبكة الإنترنت طوال إحدى عشر عاماً وفي خلال هذه الفترة واجهت الكثير من المشاكل الأمنية والإختراقات للمواقع وللأجهزة وللشبكات ، لذلك أردت بهذا الكتاب أن أوضح ما هي المشاكل الأمنية وما هي أنسب الحلول حتى نتجنب عمليات الإختراق والسرقة وخصوصاً أمن عمليات الدفع عبر الشبكة ولقد قمت بالإستعانة ببعض الكتب الإليكترونية **e-book** بالمواقع العربية والمواقع الأجنبية وقمت بإعادة صياغة بعضها علمياً لكي يتماشى مع بلادنا العربية وما يحدث لمواقعنا من إختراقات لذلك أشكر أصحاب هذه المواقع ..

لذلك محتوى الكتاب يعبر عن رأى المؤلف في هذا المجال ، بدون أدنى مسؤولية على الناشر.

## المقدمة

### حينما أصبحت ضحية الهاكرز كتبت هذا الكتاب

١. حينما كنت في أمريكا وأثناء عملي بموقع ebay وهو موقع مزاد للبيع والشراء كما تعلمون ، اخترق أحد الهاكرز ذات القبعة السوداء (الكرakers) البريد الإلكتروني الخاص بي وسرق كلمة السر وإسم المستخدم وبالتالي قام بسرقة إسم المستخدم وكلمة السر بحسابي بموقع ebay ، كل هذا وأنا لا أدري إلا بالصدفة البحتة ، حينما أفتح بريدي لا أجد أية مراسلات من العملاء ، الغريب أنني أذهب إلى ebay وأرى منتجاتي قد بيعت ولكن لا أستقبل أية مراسلات تفيد ذلك ، لم يكن في الحسبان أن وراء هذا الحدث هاكرز يهود وقد عرفتهم بعد ذلك ، فقد أرادوا إنهاء عملي بموقع ebay وسرقتي حتى أتوقف عن منافستهم ويقوموا هم فقط بالبيع عبر الشبكة. لم يكتفوا فقط عند إغلاق موقعي بل قاموا بإدراج مئات المنتجات تحت إسمي وفي خانة مواصفات الدفع كتبوا أنهم يقبلون الدفع باستخدام الشيكات والحالات money order ولكن



الحمد لله تم إكتشاف هذا اللعبة ثم أسرع وأبلغت ebay عن طريق Live Chat وهي الأسرع للإبلاغ عن السرقات والنصب وبالفعل تم إغلاق حسابي فوراً ، ثم قامت شركة ebay بفتح حسابي من جديد مع تغيير إسم المستخدم وكلمة السر .. وقد أوقعت بهم بحمد الله ورسمت لهم خطة قانونية وليست إجرامية كما فعلوا ، فقط قمت بقراءة سياسات موقع ebay جيداً وإكتشفت ثغرة هامة يمكن عن طريقها الإيقاع بأى مستخدم وغلق حسابه فوراً ، هذه الثغرة تسمى shell bidding وهذه عملية يقوم بها صديقان لهما حسابين مختلفين بموقع ebay يقوم إحداهما بالمزايدة على منتج الآخر حتى يكثروا من مبلغ المزايدة وهذه العملية إن تم رصدها بواسطة قسم الأمان والتأمين بموقع ebay فسوف يتم غلق الحسابين فوراً ونهائياً و بلا رجعة ، وقد كان ، فقد قمت بمراقبتهم وكنت أنا third party بينهم حتى تكتمل القضية ، وأبلغت ebay بأننى أحاول أن أشتري منتج من هذا المستخدم ولكن يوجد مستخدم آخر يرفع فى القيمة لحساب المستخدم الأول وتكررت هذه العملية مرات عديدة وتم رصدهم وتم إغلاق حسابهما نهائياً .. فإن كنت أنا فى هذه الحالة هاكر فأنا هاكر ذات قبعة بيضاء قمت بإبلاغ الهيئات

المختصة عن جريمة بشعة وهى جريمة السرقة التى يعاقب عليها بقطع اليد فى مذهبنا الحنيف ..

ومن هنا أنصح جميع الإخوة والأخوات العرب الذين يمكنون فى البلاد المدرجة للعمل بـ *ebay* و *paypal* كأمريكا وأوروبا وبعض دول آسيا وأستراليا وبالطبع كندا ، أن يتوخوا الحذر حين التعامل عبر مواقع *ebay* و *paypal* لأنها أكثر المواقع إختراقاً بالرغم من وجود برامج حماية شديدة ...

٢. إقتحام موقع المركز العلمى لتبسيط العلوم عن طريق دار نشر معروفة بالإسكندرية وتغيير الموقع إلى موقع آخر لمدة ساعتين ثم تيقظوا لها موظفى المركز وأغلقوا الثغرة وهو الآن يعمل بحماية جدار نارى والحمد لله ، وقد تم معرفة الهاكرز ونحن الآن نقاضيهم وسيتم الإفصاح عنهم عن قريب .

٣. ذهبت إلى أحد البنوك بالإسكندرية لفتح حساب وأودعت مبلغ معين لفتح الحساب ، وبعد أسبوعين أودعت مبلغ آخر لغرض تحويله إلى مصدر بالخارج ، وبعد شهر أرسل البنك كشف الحساب فوجدت أن الحساب ينقصه مبلغ آخر لم يتم إضافته ، ذهبت إلى البنك لأتحسس الأمر وأسأل عن ما حدث

، فوجدت موظفى البنك فى ذهول وأحسست أن شيئاً ما يجرى  
وتعالّت أصوات الموظفين وأرسلوا إلى قسم الكمبيوتر  
والمسؤولين عن حماية حساب العملاء وقد كان ما فى الحسبان ،  
لقد إخترق هاكرز حسابات البنك وأخذ مبالغ من حسابات  
العملاء وتم غلق النظام لمدة يومين لحين سد الثغرات ، وبالطبع  
تم إسترداد المبلغ الذى سرق من حسابى ...

٤. أرسل أحد أعداء النجاح شخصاً إلى مكنتى وبطريقة ما  
إكتسب ثقتى به حتى أنه قال لى إسمح لى أن أقدم لك هدية على  
جهاز الكمبيوتر الخاص بك ، فقلت له لا مانع تفضل وجلس  
أمام الجهاز وللأسف وضع المجرم دودة أو أعتقد كانت تروجان  
وتم بهذا البرنامج التعرف بل وسرقة كل ملفات الكتب  
الموجودة لدى بالجهاز ولم يكتفى بذلك بل وقد دمر الجهاز  
كليةً حتى وصل للوضع فورمات **format** والحمد لله كان  
لدى نسخة أخرى من الكتب على **CD** ، وبعد إكتشافى لهذا  
العمل الإجرامى لم أتخيل أن هناك شباب المقروض أنهم حماة  
الوطن ، هم بالفعل من سيدمر الوطن وهذا ما نراه بالفعل بين  
أوساط الشباب بنين وبنات ، معظمهم هاكرز ذات قبعة

سوداء .. لذلك لا تسمح أبداً لأى صديق قبل العدو أن يجلس على جهازك أو تعطيه كلمات السر الخاصة بك .

٥. فى هذه الأيام حدثت لى حادثة غريبة جداً : أرسل لى أحد العملاء أنه يريد شراء موسوعة التجارة الإلكترونية ، فقامت بالرد عليه ورحبت به وقلت له أرسل العنوان الخاص بك وسوف أرسل الكتب بطريقة COD الدفع عند الإستلام، وبالفعل أرسله لى وهو يقيم بإحدى قرى مصر ، أرسلت الكتب واستلم الكتب ودفع قيمة الموسوعة .. دخلت إلى بريدى الإلكتروني الخاص ببيع الكتب فوجدت رسالة يقول لى لماذا تبيع الكتب بدون أن يدفع الزبون قيمة الشحن وأحسست أنه يقو لها بنية لم ترضى ، والله أعلم .. دخلت إلى بريدى الخاص بالرد على إستفسارات أعضاء المنتدى فوجدت رسالة من هذا العميل بها مرفقات فتحت الرسالة ولكن ظهرت لى رسالة من برنامج الحماية الخاص بى يقول أن هذه الرسالة بها فيروس مدمر وطبعاً قمت بغلق الرسالة ولم أفتحها .. فدخلت إلى بريدى الثالث الخاص بالدعم الفنى للعملاء فوجدت رسالة أيضاً من هذا العميل بها مرفقات عبارة عن صور وطبعاً كانت مليئة بملفات التجسس وطبعاً لم أفتحها .. فى الحقيقة لم أنام حتى

الآن لكي أعرف ما هي اللغزة التي دخل منها هذا العميل وأخذ الإيميلات E-mails الخاصة بي ، غريب جداً ، وفي النهاية إكتشفت أن هذا العميل الذي إشتري الموسوعة أرسل لي برنامج تجسس و هذا البرنامج يرسل له جميع الحروف التي تكتب على لوحة المفاتيح الخاصة بي فعرف الإيميلات الخاصة بي من هذا الملف والله أعلم ربما يكون قد عرفها عن طريق إختراقات أخرى .. وبالطبع ما كان على إلا أن غيرت كلمات السر الخاصة بالإيميلات الثلاثة .. وأنا الآن أحاول التأكد من طريقة الإختراق قبل فعل أى إجراء قانوني ضد هذا الكراكر ..

٦. أحد أصدقائي سرق هاكركز رقم بطاقته الإئتمانية واشترى موبايل (جوال) ولم يتم الحصول على مكان الهاكرز .

٧. أحد الهاكرز تلصص إلى جهاز كمبيوتر أحد أصدقائي وكشف عن ملفاته وصوره ثم أخبره أن لديه ملف تجسس ولصدق كلامه قال له ما هي الملفات الموجودة بجهازه.

٨. لا تترك كاميرا الويب مفتوحة طوال الوقت حيث أن بعض الهاكرز يدخلون جهازك وينتهزون فرصة وجود الكاميرا

مفتوحة فيشاهدونك ، فعلى الأخوات الإنتباه إلى ذلك لأنه بالفعل تم رؤية الفتيات عن طريق برامج اختراق الملفات ...

٩. وأقوى ضحايا الهاكرز والكراريز هم المساهمين في البورصة والأسهم وما حدث ببورصة السعودية الأيام الماضية من هبوط شديد ما هو إلا بسبب اختراق الهاكرز اليهود لأنظمة البورصة السعودية والتلاعب فيها فكانت السبب في إنهارها ولكن تم السيطرة عليها ..

١٠. أتسلم كل يوم عشرات الرسائل الإلكترونية من أسماء لا أعرفها وبالطبع لا أقوم بفتحها لأنها جميعاً تحتوى على فيروسات إلا فئة قليلة قد تكون صادقة وهى تعرض إعلاناتها وخدماتها عبر بريدك الإلكتروني.. لذلك لا تقوم بفتح الرسائل الغامضة .

١١. سألتى صديقى هل لى أن أخترق أجهزة الكمبيوتر وأحذف المواقع والصور الفاضحة ، قلت له يمكنك ذلك بالرغم من أنك فى هذه الحالة تعتبر هاكر ذات قبعة بيضاء ، فضحك.

١٢. ثم سألتى وهل لى أن أخترق أى موقع جنسى وأقوم بإغلاقه ، قلت له نعم وأنت فى هذه الحالة تجاهد فى سبيل الله ..

١٣. وتتابع هل الإختراق والتجسس جريمة يحاسب عليها القانون ، قلت بالتأكيد يعد الإختراق والتجسس جريمة يحاسب عليها

القانون وذلك في الكثير من دول العالم حتى أن كل دولة الآن لديها جهاز خاص بمكافحة الإجرام عبر الإنترنت .. فلا تستغرب عزيزي القارئ حينما ترى الهاكر والكراكر بجوار القاتل ومروج المخدرات واللصوص في زنزانة واحدة ولكن الفرق بينهما هو أن القاتل إذا خرج وجد الدنيا سوداء وجميع الأبواب مغلقة أمامه ، أما بمجرد خروج الهاكر أو الكراكر من السجن يجد استقبالاً حافلاً من الشركات العالمية الكبرى التي تسارع إلى توظيف الهاكرز بغرض الاستفادة من خبرتهم في محاربة الهاكرز وكذلك للاستفادة من معلوماتهم في بناء برامج وأنظمة يعجز الهاكرز عن إقتحامها.

١٤. الخبر الأكيد أيضاً أن الهاكرز والكراكرز أصبحوا من أقوى الوسائل التي يستخدمها المنظمات الإستخبارية كالموساد الإسرائيلي والـ FBI الأمريكي لسرقة معلومات العدو وتدمير وتغيير مواقعهم بالويب كما هو الحال في كثير من المواقع الدينية التي غيرها أعداء الله إلى مواقع جنسية.

١٥. إذا الحروب الإلكترونية هي حروب هذا العصر وليست حروب ساحات القتال.

١٦. و يجب أن نؤمن بأنه لا يوجد نظام تشغيل أو جهاز بدون ثغرات أو منافذ يستطيع من خلالها الهاكرز أو الكراكرز

الإختراق ، لأنه في الحقيقة الهاكرز هم بالفعل من قام بتصميم هذه الأجهزة سواء كان بالفكرة أو بالتصميم أو عمل البرامج أو حتى بالإستشارة التقنية ، فأغلب وأقوى الهاكرز في العالم هم بالفعل مبرمجون ومهندسون للكمبيوتر والاتصال والشبكات.

١٧. وأخيراً الشباب ، الشباب ، الشباب المراهقون ، الذين يظنون أنهم يغامرون ويلهون فقط بهذه الأعمال التي لا يظنون أنها أعمال إجرامية ، لا بد من إيقافهم وعدم مساعدتهم في التلصص والتجسس والسرقة حتى لا نراهم يوماً بين القضبان .

يقول الله تعالى: " **وَلَا تَجَسَّسُوا** وَلَا يَغْتَبِ بَعْضُكُم بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَنْ يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَحِيمٌ "

سورة الحجرات الآية ١٢

واعلم أخى الشاب أن إستخدام العلم في الضرر بالناس خيانة وقد قال الله سبحانه وتعالى :

" **وَمَا تَخَافُنَ مِنْ قومِ خِيَانَتٍ** فَأَنْبِذْ إِلَيْهِمْ عَلَى سَوَاءٍ إِنَّ اللَّهَ لَا يُحِبُّ الْخَائِنِينَ "

سورة الأنفال الآية ٥٨

وبالطبع الهاكر أو الكراكر خائن لا يحبه الله ..



وفي سورة القصص الآية ٨٣ يقول الله سبحانه وتعالى:

"تلك الدار الآخرة نجعلها للذين لا يريدون علواً في الأرض ولا فساداً  
والعاقبة للمتقين"

وفي سورة المائدة الآية ٣٣ يقول الله تعالى

"إنما جزاء الذين يحاربون الله ورسوله ويسعون في الأرض فساداً أن  
يقتلوا أو يصلبوا أو تقطع أيديهم وأرجلهم من خلاف أو ينفوا من  
الأرض ذلك لهم خزي في الدنيا ولهم في الآخرة عذاب عظيم"

أما في حق السارق والسارقة قال تعالى

"والسارق والسارقة فاقطعوا أيديهما جزاء بما كسبا نكالا من الله  
والله عزيز حكيم"

سورة المائدة الآية ٣٨

## الفصل الأول

# مصطلحات امن المعلومات والمواقع والحسابات

قبل البدء في شرح مادة هذا الكتاب لابد أن نذكر بعض المفاهيم والمصطلحات التي سنتناولها طوال فصول الكتاب القادمة ، فليس من الحكمة أن نذكر علاج ووقاية قبل أن نعرف المرض وكيفية توغله داخل الجسم حتى تتمكن من التخلص منه ، من مصدره (جذوره) .

فإذا أردت أخى القارئ أخى القارئة أن تتمكنوا من حماية أجهزكم ومواقعكم من الإختراق والدمار فلا بد أن تتعلموا هذه المصطلحات أولاً حتى تعرفوا ما هو أصل العطب **fault** وحتى يمكنك سرعة المعالجة فور حدوث المشكلة أو بمعنى آخر فور الإصابة بالفيروس .

فلا يجوز أن ندخل في فصل كيفية الحماية قبل أن نتعرف مثلاً على معانى هامة مثال : الهاكر و الكراكر ومعنى الفيروس والدودة والتروجان وأيضاً مضادات الفيروسات مثال نورتون ..

لذلك في الفصل القادم نتعرف وندرس بعض المفاهيم الخاصة بأمن

المعلومات والمواقع وحماية أجهزتنا من الاختراق والثغرات والفيروسات وبذلك نكون قد جهزنا أنفسنا للدخول في فصول الكتاب وفهم مواضيعها بكل سهولة ويسر .

### – Administrator المدير

شخص يقوم بإعداد مصادر الشبكة وتسجيل المستخدمين وأرقامهم السرية وصيانة المصادر .

### - Agent عميل

في نظام العميل/الموفر (الخادم) (Client/Server) ، ذلك الجزء من النظام الذي ينفذ عملية إعداد وتبادل المعلومات نيابة عن برنامج المضيف

### Host أو الموفر Server

### - Alert تحذير

تقرير عن وجود خطأ بشكل علامة أو نافذة تحذير أو صوت يطلقه الكمبيوتر للتنبيه .

### - ASCII قاعدة المعايير الأمريكية لتبادل المعلومات

American Standard Code for Information Interchange

معياري لتحويل الأحرف إلى أرقام وتحتوي على سبعة جزئيات بقيمة ثنائية

تتراوح بين الصفر و ١٢٧ .

### - Anonymous مجهول

تم استخدامه كإسم مستخدم للدخول على بعض أجهزة الكمبيوتر البعيدة .

### - Authentication التوثيق

تعريف هوية شخص أو الإجراءات الخاصة بذلك .

### - Band Width عرض النطاق

هي كمية المعلومات التي يمكنك إرسالها على خط معين في وقت محدد. عرض النطاق يقاس بعدد النبضات في الثانية Bits per Second وتكتب (bps).

### - BBS لوحة إعلانات النظام

كمبيوتر مزود ببرامج معينة يوفر رسائل إلكترونية وملفات إضافية للخدمات الأخرى .

### - Binary ثنائي

وسيلة عد تستخدم الرقمين ٠ و ١ ، وهي الوسيلة التي يعمل بها الكمبيوتر داخلياً، وتحتوي الملفات الثنائية على ثمان جزئيات تتراوح بين صفر و ٢٥٥

### - Browser المتصفح

برنامج التصفح يستخدم للإبحار داخل شبكة الإنترنت WWW

### - Client تابع

جهاز كمبيوتر يقوم بطلب الخدمة من جهاز كمبيوتر آخر، فعندما يطلب كمبيوتر اشتراك مع مزود خدمة ISP فإنه يعتبر تابع لمزود الخدمة (Client of ISP).

### - Compression ضغط

عملية ضغط المعلومات لتخزين الملف في مساحة أصغر .

### - Connection ربط

وسيلة إتصال بين جهازي كمبيوتر .

### - Crack تحريب

مصطلح يطلق على برنامج يقوم بفك شفرة أحد البرامج المشتركة وجعله مجاني .

### - Cracker مترب

شخص يحاول الدخول على نظام ما دون تصريح ويسبب له أضرار .

### - Data بيانات

معلومات وبشكل خاص المعلومات المستخدمة بواسطة البرامج، أصغر وحدة

في المعلومة يمكن للكمبيوتر فهمها هي bit

### - Default بديل افتراضي

قيمة أو فعل أو ترتيب افتراضي يقوم الكمبيوتر بافتراضه في حال عدم قيام المستخدم بإعطاء تعليمات صريحة بخلاف ذلك.

### - Device جهاز

الأجزاء التي يتركب منها الكمبيوتر Hardware مثل الشاشة والطابعة وخلافه ، هذه الأجزاء يمكن أن يطلق عليها أيضاً الأجزاء الخارجية Peripheral لأنها منفصلة بصورتها المادية عن الكمبيوتر ولكنها مرتبطة به .

### - Dial-up اتصال

استخدام التليفون لربط الكمبيوتر بالانترنت عبر فاكس مودم. وهذا يعني أنه كي تحصل على الخدمة فإنه عليك أن تعمل مكالمات هاتفية .

### - Digital Certificates الشهادات الرقمية

تصدُر الشهادات الرقمية عن الجهات المانحة ( certificate

authorities- CA) الموثوق بها التي توقع عليها، وتستخدم هذه

الشهادات للتحقق من موثوقية المفاتيح العامة التي أُصدرت.

وفي البداية، يقوم شخص (أو شركة) بتوليد زوج من المفاتيح العامة/الخاصة،

ثم يُرسل المفتاح العام إلى جهة مائة للشهادة (CA). وتُضيف الجهة المائة (CA) بعض المعلومات المتعلقة بالشهادة (مثل: الاسم، ورقم التعريف (No ID)، وعنوان البريد الإلكتروني (Email address)، وتاريخ الانتهاء (date expiration)، والرقم التسلسلي (serial no))، وتوقع عليها بالمفتاح العام لطالب الشهادة، وبالمفتاح الخاص للجهة المائة للشهادة (CA). ويصادق توقيع الجهة المائة للشهادة (CA) على المعلومات المضافة إلى الشهادة وعلى المفتاح العام الموجود ضمن الشهادة. ويمكن أن ترسل الجهة المائة الشهادة إلى طالبها، أو تنشرها للعموم، أو تحتفظ بها في خادم الشهادات (certificate server) (قاعدة بيانات تسمح بتسليم واسترجاع الشهادات الرقمية).

### - Domain حقول

هو ذلك الجزء من الـ DNS الذي يحدد مكان شبكة كمبيوتر وموقعها في العالم .

### - DNS نظام أسماء الحقول

Domain Name System هو نظام لتحديد العناوين بالشبكة IP Addresses المطابقة للكمبيوترات المسماة والحقول Domains.. الـ DNS يتكون من سلسلة من المعلومات تفصل بينها نقاط ... خدمة أسماء الحقول Domain Name Service هي عبارة عن برنامج يقوم

بتحويل أسماء الحقول Domain Names إلى عناوين شبكية IP

Addresses.

### Digital Signature- التوقيع الرقمي

يُستخدَم التوقيع الرقمي للتأكد من أن الرسالة قد جاءت من مصدرها دون تعرضها لأي تغيير أثناء عملية النقل .

ويمكن للمرسل استخدام المفتاح الخاص لتوقيع الوثيقة إلكترونياً. أما في طرف المستقبل، فيتم التحقق من صحة التوقيع عن طريق استخدام المفتاح العام المناسب.

### Electronic Mail- البريد الإلكتروني

يرمز له e-mail وهو نظام يمكن بموجبه لمستخدم الكمبيوتر تبادل الرسائل مع مستخدم آخر أو مجموعة مستخدمين بواسطة شبكة الإنترنت، ويحتاج البريد الإلكتروني إلى برنامج بريد مثل Outlook: أو Eudora ليتمكن من الإرسال أو يعمل تحت برامج مجانية لمواقع مثل yahoo .

### Emotion- رموز المشاعر أو الأحاسيس

رموز تستخدم للتعبير عن المشاعر على الانترنت مثل إبتسامة ، غضب ، حزن ، سعادة

### Encryption- التشفير



هو معالجة كتلة من المعلومات بهدف منع أي شخص من قراءة تلك المعلومة باستثناء الشخص المقصود إرسالها إليه، وهناك العديد من أنواع التشفير .

و يُعرَّف التشفير بأنه عملية تحويل المعلومات إلى شيفرات غير مفهومة (تبدو غير ذات معنى) لمنع الأشخاص غير المُرخَّص لهم من الاطلاع على المعلومات أو فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مُشفَّرة.

### - FAQs الاستلث المتكررة

**Frequently Asked Questions** وثيقة على الانترنت الغرض منها فحص وتدقيق المعلومات التي يحتاج إليها الكثير من الأشخاص بصفة متكررة .

### - Firewall جدار نار

نظام تأمين لتقييد عملية الدخول على أجهزة الكمبيوتر الموجودة على شبكة محلية LAN من أي مكان في الخارج .

### - Flame التطهير

ردة فعل غاضبة لرسالة تم نشرها على Usenet أو القوائم البريدية Mailing List أو لوحات النقاش Message Boards ، التطهير يحدث لعدة أسباب مثل تعميم رسالة على الانترنت أو طرح سؤال توجد

إجابته في الـ FAQs ، حرب التطهير قد تحدث عندما يرد شخص تعرض للتطهير على الرسالة أو الرسائل التي وصلته .

### - Gateway بوابة

مصطلح بوابة Gateway البوابة هي أداة أو برنامج اتصال يقوم بتسيير المعلومات من شبكة إلى أخرى .

### - Gopher خدمت جوفر

نظام طورته جامعة مينيسوتا الأمريكية بهدف تسهيل عملية استخدام الانترنت وهو يعتمد على عملية البحث من خلال القوائم لقراءة الوثائق ونقل الملفات Gopher يمكنه الإشارة الى الملفات ومواقع Telnet ومراكز معلومات WAIS وغيرها .

### - Hacker متطفل

المتطفل هو الشخص الذي يشعر بالفخر لمعرفته بطرق العمل الداخلية للنظام أو الكمبيوتر أو الشبكات بحيث يسعى للدخول عليها دون تصريح .

### - Host مضيف

غالباً ما يستخدم مصطلح مضيف Host للكمبيوتر الذي يتيح للمستخدمين الدخول عليه .

### - HTTP بروتوكول نقل النص التشعبي

HTTP هي وسيلة تجعل من الممكن التصفح عبر وثائق الشبكة العنكبوتية، المستخدم يضغط على وصلات ربط موجودة على وثيقة الشبكة العنكبوتية مما يمكنه من الذهاب إلى تلك الوثيقة حتى لو كانت موجودة على جهاز آخر .

### - ISDN الشبكة الرقمية للخدمات الموحدة

Integrated Services Digital Network هي تكنولوجيا جديدة تحتوي على شبكات صوتية ورقمية في وسيلة واحدة وتعتبر خدمة اتصالات فائقة السرعة ولكن وجود DSL حزم من استعمالها .

### - IP بروتوكول الانترنت

Internet Protocol هو طبقة الشبكة الخاصة ببروتوكول TCP/IP والتي تستخدمها الأدوات على الانترنت للاتصال ببعضها. والـ IP Address عنوان بروتوكول الانترنت، هو العنوان الخاص بكل كمبيوتر متصل بشبكة ولكل عنوان الـ IP طريقتين للكتابة اما رقمية (TCP/IP Address) مثل ١٩٢،١٦٨،٢٣،١ أو حرفية (FQDN) وهي العناوين التي نكتبها عادة في المتصفحات مثل ftp.books4internet.com والعنوان الحقيقي هو الرقمي ولكن لصعوبة حفظه فنكتب العنوان الحرفي ولكن في الشبكة داخليا يتم ترجمة العنوان الحرفي الى العنوان الرقمي المطابق له .

- ISP مزود خدمة الانترنت

Internet Service Provider هو الشركة التي يقوم المستخدم -

عادة - بالاشتراك لديها للحصول على ربط بالانترنت، وهذه الشركة

مرتبطة بالانترنت مباشرة من إحدى الشركات الأعضاء في CIX

JPEG

وسيلة لضغط الصور المستخدمة في الانترنت ويكون إمتداد إسم الصورة

هو .jpeg

- Kilobit كيلو بت

وحدة قياس تعادل ١٠٢٤ ب، وتستخدم عادة في تحديد الطاقة الاستيعابية

للذاكرة

- Kilobyte كيلو بايت

وحدة قياس تساوى ١٠٢٤ بايت .

- Layer طبقة

شبكات الكمبيوتر قد تنظم على شكل مجموعة أعداد أكثر أو أقل من

البروتوكولات المستقلة كل منها في طبقة Layer وقد تسمى مستوى

Level.

**Login تسجيل -**

أي أن تقوم بتسجيل إسمك كمستخدم لنظام أو شبكة فيصبح لديك اسم مستخدم **Login Name.**

**Log off انتهاء عملية التسجيل -**

هو إخبار النظام بأنك أنهيت عملك وستقطع الإتصال.

**Lurking التواري -**

يستخدم هذا المصطلح للتعبير عن شخص ليس لديه مشاركة نشطة في مجموعة الاخبار او لوحة النقاش أو قائمة البريد التي اشترك معها، ويفضل التواري للأشخاص المبتدئين الذين يريدون التأقلم في البداية مع الآخرين

**Mailing List قائمة بريدية -**

قائمة بعناوين اليكترونية لعدة أشخاص. كل شخص مشترك في هذه القائمة يرسل موضوعاً يخص اهتمامات هذه القائمة الى كمبيوتر رئيسي يقوم بتحويل هذه الرسالة الى جميع المشتركين في القائمة البريدية، هناك قوائم معدلة **Moderated** وتعني أن الرسالة ترسل في البداية الى صاحب هذه القائمة ليدقق فيها وإذا تأكد من صلاحيتها يقوم بارساله للبقية وهناك قوائم غير معدلة **Immoderate** وتقوم بارسال الرسالة أوتوماتيكياً للمشاركين .

**Megabyte - ميجا بايت**

وحدة قياس تعادل ١٠٢٤ كيلو بايت أو ١٠٤٨٥٧٦ بايت .

**MIME - توصيلت بريد الانترنت المتعددة الأغراض****Multipurpose Internet Mail Extension**

القدرة على نقل البيانات غير النصية كالصور والصوت والفاكس من خلال البريد الالكتروني .

**Message digests البصمة الإلكترونية للرسالة**

رغم أن التشفير يمنع المتلصّصين من الاطلاع على محتويات الرسالة، إلا أنه لا يمنع المخربّين من العبث بها؛ أي إن التشفير لا يضمن سلامة الرسالة (integrity). ومن هنا ظهرت الحاجة إلى البصمة الإلكترونية للرسالة (message digest)، وهي بصمة رقمية يتم اشتقاقها وفقاً لخوارزميات معينة تُدعى دوال أو اقترانات الترميز (hash functions)، إذ تطبّق هذه الخوارزميات حسابات رياضية على الرسالة لتوليد بصمة (سلسلة صغيرة) تمثّل ملفاً كاملاً أو رسالة (سلسلة كبيرة). وتُدعى البيانات الناتجة البصمة الإلكترونية للرسالة.

**MD5، MD2، MD4 خوارزميات البصمة الإلكترونية**

طوّر رونالد رايڤست (Ronald Rivest) خوارزميات **MD2** و **MD4** و **MD5** الخاصة بالبصمة الإلكترونية للرسالة. وهذه

الخوارزميات هي اقتراحات تمويه يمكن تطبيقها على التوقيعات الرقمية. وبدأ ظهور هذه الخوارزميات عام ١٩٨٩ بخوارزمية MD2، ثم تلتها خوارزمية MD4 عام ١٩٩٠، ثم خوارزمية MD5 عام ١٩٩١.

أكثر هذه الخوارزميات أماناً هي MD5؛ وهي تستند أساساً إلى خوارزمية MD4 مضافاً إليها بعض خصائص الأمان الأكثر إحكاماً.

### - Netiquette آداب الشبكات

الالتزام بقواعد سلوك وآداب ملائمة عند استخدام الشبكة

### - NETBIOS نظام شبكات المدخلات والمخرجات الأساسي

Network Basic Input/Output System يسمح للأجهزة

التي تعمل بنظام DOS من التحدث مع واستعمال خدمات الشبكة. نفس

الاسم هو اسم بروتوكول شبكة محلية يستخدم بشكل واسع في منتجات

ميكروسوفت .

### - Newsgroup مجموعات اخبار

مجموعات الأخبار التي قد يصل عددها الى ٢٠,٠٠٠ مجموعة تكون معاً

الـ Usenet، وهي بمثابة الصحف التي تناقش جميع موضوعات الحياة وأي

موضوع قد يخطر ببالك، ومعظم موفري الخدمة يوجد لديهم موفر مجموعات

أخبار Newsgroup Server

**On-Line/Off-Line متصل/غير متصل** -  
**On-Line** تعني أن الكمبيوتر متصل حالياً بالشبكة وعكسه **Off-Line** أي غير متصل .

**PING** - مجمع كتلت الانترنت  
**Packet Internet Grouper** برنامج يستخدم لاختبار القدرة  
 الوصلية وذلك بارسال طلب صدى **ICMP** إليها وانتظار الرد

**PPP** - بروتوكول نقطتي الى نقطتي  
**Point-to-Point Protocol** إحدى وسيلتين لتبادل كتل البيانات  
 عبر انترنت بواسطة خطوط الهاتف ( الوسيلة الأخرى هي **SLIP** )  
**PPP** يوفر وسيلة ضغط للبيانات وتصحيح الأخطاء ولا يزال  
 تحت التطوير .

**POP** - بروتوكول مكتب البريد  
**Post Office Protocol** يسمح للمستخدم بتخزين رسائله في  
 كمبيوتر شركة توفير الخدمة كي يقوم باسترجاعها فيما بعد، وهناك ثلاث  
 طبقات لهذا النظام **POP** و **POP2** و **POP3** .

**Port** - ميناء (منفذ)



تحديد موقع برنامج معين على كمبيوتر مضيف على الانترنت.. قبل سنوات قليلة كان على المستخدم تحديد البورت بنفسه؛ المنفذ ٢٣ خاص بالـ Telnet والمنفذ ٢١ خاص بالـ FTP، أما اليوم فمعظم البرامج تحدد البورت أوتوماتيكياً .

### – Proxy نفويض

طريقة يقوم بمقتضاها جهاز -- موجه غالباً -- بالرد على طلبات للدخول على مواقع معينة وبذلك يقوم بتنفيذ هذا الطلب بناء على الأوامر التي تلقاها وعلى التوجيه الذي صُمم عليه .

### - Queue صف

كتل احتياطية تنتظر المعالجة

### - RAM ذاكرة الدخول العشوائي

Random - Access Memory الجزء من ذاكرة الكمبيوتر الذي يقوم بتخزين المعلومات بصفة مؤقتة بينما هي تحت الاستخدام. أغلب أجهزة الكمبيوتر تحتوي على ٥١٢ كيلوبايت من ذاكرة الرام، هذه المعلومات اذا أغلقت الجهاز ولم تحفظها تختفي بلا رجعة .

### – Remote بعيد

لا يمكن ربطه مباشرة باستخدام أسلاك محلية ولكنه يحتاج الى أدوات اتصال

أخرى wireless .

### - Router موجه

نظام كمبيوتر يتخذ القرارات الخاصة بتحديد اتجاهات الحركة على الانترنت وهو ما يستخدمه أصحاب مقاهي الإنترنت لتوصيل أكثر من جهاز بالإنترنت .

### - SLIP بروتوكول الانترنت ذو الخط المتسلسل

Serial Line Internet Protocol هو بروتوكول يستخدم لتشغيل بروتوكول الانترنت IP على خطوط متسلسلة Serial Lines كدوائر الهاتف. عادة عند الارتباط بموفر خدمة يستخدم اما PPP أو SLIP.

### - Server خادم (موفر)

جهاز يفتح للمستخدمين لتوفير الخدمات لهم كنقل الملفات وغيرها .. الشخص الذي يدخل على الـ Server يسمى Client

### - Shell المطهرة

برنامج يوفر للمستخدم القدرة على التفاعل مع الكمبيوتر .

### - SMTP بروتوكول نقل البريد البسيط

بروتوكول يستخدم لنقل البريد الالكتروني بين الأجهزة .

## - Spamming التعميم

مصطلح يطلق على عملية تعميم رسالة في مجموعات الأخبار أو البريد الإلكتروني وهي في الغالب رسائل غير مرغوب فيها ويقول عنها البعض أنها رسائل الغرض منها نصب أو الإعلان. ويقابله التطهير **Flaming**

## - Standard معيار (افتراضي)

مجموعة من المواصفات لتصميم البرامج يتم الاعتراف بها من قبل بائعين أو منظمة رسمية دولية .

## - Digital Signature التوقيع الرقمي

يُستخدَم التوقيع الرقمي للتأكد من أن الرسالة قد جاءت من مصدرها دون تعرضها لأي تغيير أثناء عملية النقل. ويمكن للمرسل استخدام المفتاح الخاص لتوقيع الوثيقة إلكترونياً. أما في طرف المستقبل، فيتم التحقق من صحة التوقيع عن طريق استخدام المفتاح العام المناسب.

## - SSL بروتوكول الطبقات الأمان

هو اختصار لـ Secure Sockets Layer وهذا البروتوكول هو المسؤول عن إدارة أمن الإنترنت

## T1-

مصطلح AT&T يعبر عن وسائل النقل الرقمية Digital التي تستخدم لنقل DS-1 الاشارات الرقمية المشكلة وذلك بسرعة ١,٥ MB في الثانية سرعة خارقة وذلك باستخدام خط مؤجر Leased Line وهناك أيضاً T3 التي تستخدم لنقل DS-3 بسرعة ٤٤,٧٤٦ MB في الثانية .

## TCP - بروتوكول التحكم بالنقل

يقوم هذا البروتوكول بتمرير المعلومات الى بروتوكول الانترنت IP وهو مسئول عن التأكد من وصول الرسالة وأنها مفهومة .

## Telenet - الاتصال عن بعد

Telnet هي بروتوكول إنترنت معياري لخدمات الربط عن بعد ويسمح للمستخدم بربط جهازه على كمبيوتر مضيف جاعلاً جهازه وكأنه جزء من ذلك الكمبيوتر البعيد .

فإن كنت من هواة الإبحار في آفاق الويب بحثاً عن مواقع جديدة ومثيرة في العديد من محركات البحث، ولكن إن كنت من هواة المطالعة وتقصد في بحثك المكتبات العامة ومكتبات الجامعات، فإنك ستفاجأ عند محاولة النفاذ إلى مثل هذه المواقع على الويب برسالة مفادها: "لا يُمكنك الدخول" (Access is denied)، وربما يظن الباحث أن هناك خطأ ما في الإنترنت ولكن الحقيقة مغايرة لهذه النتيجة، إذ إن النفاذ إلى هذه المواقع

يحتاج إلى خدمة أخرى من خدمات الإنترنت، تُدعى خدمة تِلنِت (Telnet)، تُحقق ما عجزت عن تحقيقه مُستعرضات الويب (Web browsers)، وقد ظهرت هذه الخدمة في أوائل السبعينات مع بداية مسيرة تطور الإنترنت، وقد وفرت كمّاً كبيراً من المعلومات التي لا يُمكن الوصول إليها عادةً على شبكة الويب العالمية.

### - Trojan horse حصان طروادة

برنامج كمبيوتر يحمل داخله وسائل تسمح بالدخول الى النظام الذي زُرِعَ فيه .

### - URL معين المصادر المنتظم

Uniform Resource Locator وسيلة معيارية للإشارة للمصادر تقوم بتحديد نوع الخدمة بالإضافة إلى موقع الملف أو الدليل .

### - Unix نظام يونيكس

نظام تشغيل تستخدمه معظم شركات توفير الخدمة ويقوم بربط عدة أجهزة تابعة Clients به للدخول عليه .

### - Usenet شبكة المستخدم

شبكة من مجموعات الأخبار تتكون من ١٦,٠٠٠ مجموعة أخبار قتم بجميع شؤون الحياة .

**- Virus فيروس**

برنامج يكرر ويضاعف نفسه عن طريق دمج نفسه بالبرامج الأخرى ويضر الكمبيوتر وملفاته المخزنة بداخله .

**- White Pages الصفحات البيضاء**

مراكز معلومات توفر خدمات ومعلومات عن أشخاص معينين تماماً مثال دلائل يلو بيدجز .

**- Whois**

برنامج يتيح لمستخدمه البحث في مراكز المعلومات عن أشخاص وعناوين وهو أيضاً موقع هام [www.whois.com](http://www.whois.com) لمعرفة من صاحب موقع ما بشبكة الإنترنت وتاريخ إشتراكه وإنهاء صلاحيته ومن السيفر المضيف وكلمات البحث المدرجة بالموقع ، فمثلاً إن أردت معرفة من هو صاحب موقع [www.books4internet.com](http://www.books4internet.com) فعليك الذهاب إلى موقع whois وإدخال الموقع ستجد تاريخ هذا الموقع .

**- WAIS**

نظام يتيح لمستخدمه البحث عن موضوع معين باستخدام كلمات إفتاحية

**Keywords.****- WWW الشبكة العنكبوتية العالمية**

برنامج يعمل باستخدام نقاط ربط Hypertext link كي يتمكن

المستخدم من التصفح بواسطة النقر على الروابط .

### - Worm دودة

برنامج يكرر نفسه ولكنه يتكاثر في الشبكة بشكل مقصود بعكس الفيروسات، دود الانترنت الذي حدث عام ١٩٨٨ ربما يكون الأشهر فقد استطاع الدود أن يتكاثر في أكثر من ٦٠٠٠ نظام .

### - WYSIWYG ما تراه هو ما تحصل عليه

What You See Is What You Get هو مصطلح يطلق على بعض برامج تصميم صفحات الويب التي تتيح رؤية ما ستكون الصفحة عليه من خلال البرنامج نفسه مثال برنامج فرونت بيج .

### - Modem- X و Modem- Y و Modem- Z

بروتوكولات تستخدم لنقل الملفات بين حاسبين عادة بواسطة مودم .

### - Zone نطاق

مجموعة من أدوات الشبكة Apple Talk

### - Zip code

الرقم البريدي Postal code وهو عبارة عن خمسة أرقام تميز كل

منطقة أو حي حتى يتم العثور على العنوان بسهولة.

## الفصل الثاني

### أمن المعلومات

لقد أعجبني كثيراً مقالاً بموقع القانون العربي يُعرف أمن المعلومات من :

منظور أكاديمي :

هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها .

ومن منظور تقني :

هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية .

ومن منظور قانوني :

فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة ، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها ( جرائم



الكمبيوتر والإنترنت) .

وإستخدام اصطلاح أمن المعلومات **Information Security** وإن كان استخداماً قديماً سابقاً لولادة وسائل تكنولوجيا المعلومات ، إلا أنه وجد استخداماه الشائع بل والفعلي ، في نطاق أنشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال ، اذ مع شيوع الوسائل التقنية لمعالجة وتخزين البيانات وتداولها والتفاعل معها عبر شبكات المعلومات- وتحديداً الإنترنت - إحتلت أبحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة ، بل ربما أمست أحد الهواجس التي تؤرق مختلف الجهات ، لدرجة أن كل جهاز أمن بكل دولة الآن أنشأت قسم خاص لمكافحة الإجرام عبر الإنترنت حتى تساعد على تقليل هذه الجرائم بل والتخلص منها إن أمكن.

**ولأن الإنترنت** تضم مجموعة كبيرة من الشبكات حول العالم وبالطبع لها فوائد كثيرة ، وأصبحت وسيلة سهلة وممتعة تُتيح للملايين البشر الحصول على كم هائل من المعلومات، إضافةً إلى التواصل وتبادل المعلومات والرسائل فيما بينهم. ولكن بعض العوامل (مثل الطبيعة المفتوحة لهذه الشبكة، وعدم وجود أي جهة يمكنها الادعاء بأنها تمتلكها أو تسيطر عليها، وعدم وجود قوانين مركزية رادعة)- أدّت إلى انتشار العديد من الجرائم على الشبكة) مثل: التجسس على حُرُم الرسائل

(packet sniffing)، وكذلك تخريب أجهزة الكمبيوتر وملفاتهما (computer hacking)، وسن هجوم الفيروسات على البريد الإلكتروني، إضافة إلى عمليات الخداع (hoaxes) وغيرها. ورغم أن الإنترنت ليست البيئة الوحيدة التي تحدث فيها الجرائم والمخالفات القانونية، إذ إن الجريمة ظاهرة موجودة في مجتمعات عديدة، فإن المشكلة الرئيسية تكمن في عدم وجود قوانين دائمة وراذعة تحمي مستخدمي الإنترنت. وما سبق نجد أن أمن الإنترنت أصبح شأنًا مهمًا لا بد من حل مشاكله، نظرا لأهمية هذا الأمن في عمليات تبادل المعلومات الشخصية ومعلومات العمل.

وتشكل قضايا الأمن والتهديدات الناتجة عنها العائق الأكبر أمام اكتساب ثقة الناس ومشاركتهم في تقدم الإنترنت من حيث حركات البيع والشراء عبر شبكة الإنترنت وإجراء الحركات المالية عبرها. وتبقى مسألة الحفاظ على أمن الإنترنت باعتماد وسائل سهلة واقتصادية من أكثر المسائل التي تشكل حالياً تحدياً كبيراً لهذه التقنية.

لذلك فإن أغراض أبحاث واستراتيجيات ووسائل أمن المعلومات - سواء من الناحية التقنية أو الأدائية - وكذا هدف التدابير التشريعية في هذا الحقل ، و هدف جميع مستخدمي الإنترنت في

الحصول على المعلومات ونقلها بشكل آمن ، ولضمان نقل آمن للمعلومات بين الأطراف المتصلة ، لابد من ضمان توفر العناصر التالية لأية معلومات يراد توفير الحماية الكافية لها :-

- السرية أو الموثوقية **CONFIDENTIALITY** : وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.
- التكاملية وسلامة المحتوى **INTEGRITY** : التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغييره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع .
- إستمرارية تـوفر المعلومات أو الخدمة **AVAILABILITY** :- التأكد من إستمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وإن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها .
- عدم إنكار التصرف المرتبط بالمعلومات ممن قام به -Non

**repudiation** :- ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها إنكار أنه هو الذي قام بهذا التصرف ، بحيث تتوفر قدرة إثبات أن تصرفاً ما قد تم من شخص ما في وقت معين .

وقد تم وضع عناصر ثلاث بنفس الكيفية مع اختلاف المسميات وهي:

- الخصوصية (privacy)،
- وسلامة المعلومات (Integrity)،
- والتحقق من هوية الأطراف الأخرى ( peer authentication)

### الخصوصية (privacy)

كي تتم المحافظة على خصوصية الرسالة الإلكترونية، يجب ألا يتمكن من الاطلاع عليها إلا الأطراف المعنية المسموح لها بذلك. وللحفاظ على الخصوصية، لا بُدَّ من التحكم بعملية الدخول، وأكثر طرق التحكم انتشاراً هي: استخدام كلمات المرور (passwords)، والجدار الناري (firewall)، إضافة إلى شهادات الترخيص (authorization certificates) مثال BBB الأمريكية.

و BBB ترمز إلى Business better bureau وهي هيئة أمريكية ، إذا حصل أى صاحب موقع تجارى على هذه الشهادة سيجنى من المال الكثير وذلك لأن هذه الشهادة بمقتضاها يدخل المشتري أو الزبون customer وهو متأكد ١٠٠% أنه لن ينصب عليه وذلك لوجود شهادة الـ BBB ، وتجند هذه الشهادة بنهاية الموقع .. وطبعاً للحصول هلى هذه الشهادة لابد من توفر شروط أمنية security وآمنة safe لصاحب الموقع وهذه الشهادة مثل شهادة الأيزو ISO التى تجعل المستوردين يشترون من المصنع الحاصل على هذه الشهادة بكل إطمئنان ..

أذكر أن أحد أصدقائى فى نيوجرسى يملك موقع مزاد ولكن كان فى بدايته ، فكان الأمر شاق عليه لكى يبيع وينافس أصحاب مواقع المزايدات الأخرى ، فاجتهد وحارب حتى حصل على شهادة BBB التى كانت بداية طيبة له حيث زادت وشجعت العملاء للشراء والبيع من خلال موقعه ..

## سلامة المعلومات (Integrity)

لا بُدَّ من حماية عمليتي نقل المعلومات وتخزينها، وذلك لمنع أي تغيير للمحتوى بشكل متعمد أو غير مُتعمد. وتكمن أهمية ذلك في الحفاظ

على محتوى مفيد وموثوق به. وفي الغالب، تكون الأخطاء البشرية وعمليات العبث المقصود هي السبب في تلف أو تشويه البيانات. وينتج عن ذلك أن تصبح البيانات عديمة الجدوى، وغير آمنة للاستخدام.

ولتلافي تشويه أو تلف البيانات، يُمكن استخدام تقنيات مثل: البصمة الإلكترونية للرسالة (message digest) والتشفير (encryption)، ومن المفيد أيضاً استخدام برمجيات مضادة للفيروسات (anti-virus software) لحماية أجهزة التخزين من انتهاكات الفيروسات التي تتسبب في تلف أو تشويه البيانات. ومن المهم أيضاً الاحتفاظ بنسخ احتياطية (backup) لاسترداد البيانات المفقودة في حال تعرضها للضرر، أو في حال تعطل الشبكة أثناء عملية النقل.

### التحقق من هوية الأطراف الأخرى (Peer Authentication)

يجب التأكد من هوية الأطراف المعنية بعملية تبادل البيانات، إذ يجب على كلا الطرفين معرفة هوية الآخر لتجنب أي شكل من أشكال الخداع (مثل عمليات التزوير وانتحال الشخصيات). وهناك بعض الحلول والإجراءات للتحقق من هوية الأطراف المتصلة مثل: كلمات

المروور (passwords)، والتواقيع الرقمية (digital signatures)، والشهادات الرقمية (digital certificates) التي يُصدرها طرف ثالث. ويُمكن أيضا تعزيز الأمن بالاعتماد على بعض المميزات المحسوسة مثل: بصمة الإصبع (print finger)، والصوت، إضافة إلى الصورة.

### امن المعلومات في المؤسسات التعليمية

يتعرض العديد من شبكات الحاسب الآلي إلى عمليات هجوم واختراقات بسبب السطو على المعلومات أو التخريب بما في ذلك شبكات المؤسسات التعليمية، وكلما كانت المعلومات هامة وحساسة كلما زاد اهتمام المخربين والمخترقين بها، مما يستدعي وجوب أخذ التدابير اللازمة لحماية المعلومات والشبكات، وقد ازداد اهتمام التقنيين بهذا الجانب مع زيادة الهجمات على الشبكات والسطو على المعلومات إلى أن أصبح أمن المعلومات تخصصا منفردا ضمن مجالات الحاسب الآلي، كما أصبح له شركات خاصة تقوم بإنتاج نظم وعتاد الحماية ووضع الحلول الشاملة له.

## الفصل الثالث

### الهاكرز و الكراكرز

البعض منا يعتقد أن كلمة ( هاكرز ) كلمة سيئة و مضمونها سيئ ، و هذا سببه أن البعض لا يعلم معنى كلمة ( هاكرز ) و في أغلب الأوقات البعض منا يخلط بين كلمة ( هاكرز ) و كلمة ( كراكرز ) ، إذاً علينا أن نعرف من هم الهاكرز ، و من هم الكراكرز ، و ما الفرق بينهما .

#### أولاً : من هم الهاكرز ؟

كلمة ( الهاكرز ) ليست كما يظن كثير من الناس أنهم أناس أشرار يقومون بالتخريب والتدمير والإقتحام المغرض ولكن هي كلمة تحمل معنى آخر وهو ( مبتكر لنظم المعلومات و البرمجيات ) فالهاكرز هم على مستوى عالٍ وتقني حتى يمكنهم ذلك من فك الشفرات والثغرات التي قد بل بالفعل تؤذى كثير من الهيئات والشبكات ، و هي أيضاً عبارة عن إسم إختاره لأنفسهم مجموعة من المبرمجين الأكفاء المهرة القادرين على ابتكار البرمج و القادرين أيضاً على حل مشكلات البرامج في الحاسب الآلي في جميع أنظمتهم و التعامل مع جميع شبكات الحاسب الآلي و يتقنون على الأقل أربع لغات من لغات البرمجة المعروفة ، و هذا مما يجعلهم يستطيعون إكتشاف الثغرات و الأخطاء في الأنظمة و الشبكات



و العمل على تلاشيها و تصحيحها ، فـ ( الهاكرز ) هم الذين صنعوا أغلب برامج الحاسبات و الشبكات و البرمجيات ، و الدلالة على ذلك أنه يجب أن نعلم أن أشهر ( الهاكرز ) حتى الآن هو ( تيرور فالدس لينوس ) أحد أهم متطورين نظام التشغيل ( Unix ) أول نظام حاسبات عرفه العالم سنة ( ١٩٧١ ) تقريباً ، و هو أيضاً المبتكر لنظام التشغيل الأكثر أماناً و تطوراً و شهرة في العالم و هو نظام التشغيل ( Linux ) ، و قد بدأ ظهور ( الهاكرز ) أثناء الحرب العالمية الثانية و كانوا في هذا الوقت يعملون مع الجيوش لفك شفرات إشارات الأجهزة اللاسلكية للجيوش الأخرى بدقة و سرعة كبيرة جداً ، ثم بعد ذلك أنتشر ( الهاكرز ) أو المبرمجين بعد إنتهاء الحرب العالمية الثانية ، و عند إختراع أول جهاز حاسب آلي ، كان لابد له من نظام تشغيل و من هنا بدأ دور الهاكرز في الظهور و البرمجة و الابتكار .

## ثانياً : من هم الكراكرز ؟

كلمة ( كراكر ) & ( Cracker ) هي كلمة بالإنجليزية تعني ( الكسر أو التكسير ) و معناها العام بالنسبة لموضوعنا أن ( الكراكرز ) كلمة تعني التخريب والعبث و التخطيم ، و هي عبارة عن إسم إختاره لأنفسهم مجموعة من المخربين المهرة القادرين على إختراق أي شبكة أو أي جهاز حاسب ، و لكن يجب أن نعلم أن إختراق المواقع الإسرائيلية

و الشبكات الإسرائيلية التي تقدم مواقع إباحية وجنسية و جميع أنواع البريد الإلكتروني الإسرائيلي spam e-mail من قبل العرب و المسلمين لا يعتبر هذا كراكر لأنه يستهدف دولة معينة أو فئة معينة ، و إنما يعتبر هذا أمر واجب علينا جميعاً ، لأن هذا جهاد و حرب ، و حتى نحاول بقدر المستطاع أن نظهر كل أماكن ومواقع الإنترنت من كل أفاعيل أعداء الله و حتى يتعظوا و يعلموا أننا قوة لا يستهان بها عند اتحادها ، فالكراكرز لا يقلون مهارة ولا كفاءة عن ( الهاكرز ) ، و لكنهم على العكس تماماً يستخدمون هذه المهارة في التخريب و السرقة و الحصول على الأموال بطريقة غير مشروعة ، و لعلنا نذكر أن من أشهر ( الهاكرز ) في العالم ( كيفن ميتيك ) الذي أصبح أسطورة في الكراكرز و أصبح هو مثلهم الأعلى ، نظراً لموهبته و قدرته الفائقة في السرقة و تدمير الأجهزة و الشبكات و المواقع بشكل عام ، و قد أصبح ( كيفن ميتيك ) أشهر ( كراكرز ) بعدما نفذ أكبر عملية سرقة تاريخية إلكترونية عرفها العالم ، حيث قام بسرقة حوالي أكثر من ٢٠٠٠٠٠ أو مائتان ألف رقم لبطاقات إئتمان سنة ( ١٩٩٥ ) ، و قد بدأ ظهور ( الكراكرز ) تقريباً بعد الحرب العالمية الثانية في حين كان ( الهاكرز ) يعملون مع الجيوش ، كانوا هم مخبئين و يخططون و يدبرون لعملياتهم اللصوية و كانت أهم اهتماماتهم في ذلك الوقت التصنت والتجسس على التليفونات والأجهزة اللاسلكية وكان هذا في أول

الأمر على سبيل المتعة وهذا باختصار كل شيء عن (الكراكر).

ما هو الفرق بين الهاكر والكراكر؟

في الحقيقة مما سبق يتضح لنا أن الفارق هو فارق أخلاقي وليس فارق علمي.

الهاكر : هو الشخص الذي يعرف عدة لغات معرفة جيدة بحيث يكون له القدره على كتابه برامج مفيده و مبتكره

إذا فالهاكر يخترع ويبتكر .

الكراكر : هو الشخص الذي يحاول بطرق غير شرعيه أن يدخل أو يدمر

الأمن للنظام أو الشبكة بنية خبيثه

و الكراكر يخرب ويسرق

و بعض الأحيان يطلقون عليهم هاكر ذو القبعه السوداء

**( Black hat hacker)**

أما الشخص الذي يحاول أن يدخل على النظام أو الشبكة بغرض مساعدة

صاحب النظام بأن يحذره بأن هناك عيوب في أمن النظام فيطلق عليهم هاكر

ذو القبعه البيضاء

**(White hat hacker)**

## الفصل الرابع

### أنواع الهجوم والإختراق Types of Attack

#### ١. التصنت على الرسائل Interception Attacks:

في هذه الحالة يقوم المهاجم بمراقبة الإتصال بين المرسل والمستقبل للحصول على المعلومات السرية وهو ما يسمى بالتصنت على الإتصال (Eavesdropping).

#### ٢. هجوم للإيقاف Interruption Attacks:

وهذا النوع يعتمد على قطع قناة الاتصال لإيقاف الرسالة أو البيانات من الوصول إلى المستقبل وهو ما يسمى أيضا برفض الخدمة (Denial of service).

#### ٣. تعديل محتوى الرسالة Modification Attacks:

وهنا يتدخل المهاجم بين المرسل والمستقبل (يعتبر وسيط بين المرسل والمستقبل) وعندما تصل إلى الـ **Attacker** فإنه يقوم بتغيير محتوى الرسالة ومن ثم إرسالها إلى المستقبل ، والمستقبل طبعاً لا يعلم بتعديل الرسالة من قبل الـ **Attacker** فيقوم بإعطاء معلومات سرية إلى

المهاجم.

## ٤. الرسائل المزورة :Fabrication Attacks

وهنا يرسل المهاجم رسالة مفادها أنه صديقه ويطلب منه معلومات أو كلمات سرية خاصة بالشركة مثلاً .

## واعلم أن أسهل طرق الإغتراف هي :

١. عن طريق المتصفح الإلكتروني إذا لم تتم ترقيةه باستمرار حيث يستطيع الهاكر دخول جهازك عن طريق متصفحك بواسطة سكربت معين ومعروف بين أوساط الهاكرز والمبرمجين.

٢. عن طريق البريد الإلكتروني عند إرسال مرفقات تروجان أو فيروسات مع البريد.

٣. عن طريق استعمال برامج المحادثة مثل الماسنجر و ICQ و MIRC وهذه البرامج يستخدمها كثير من الضحايا.

٤. عدم ضبط إعدادات المتصفح حتى يمنع دخول الكوكيز الغير آمنه إلى الجهاز.

٥. عدم ترقية نظام الويندوز المستخدم بانتظام حيث يتم إكتشاف ثغرات أمنيته في النظام من قبل شركة مايكروسوفت.

٦. تنزيل البرامج باستمرار دون التأكد من نظافتها من التروجان والفيروسات والكارثة عند البحث عن الكراك لتلك البرامج في مواقع الهاكرز المغمه بالإسكربت الذي يخرق المتصفح والدخول لجهاز الضحية.

٧. عدم وجود برامج حمايه يتم ترقيتها باستمرار.

## الإجراءات المضادة للتهديد Threats أو الهجوم: Attacks

- وضع جدران نارية Firewalls
- برامج مكافحة الفيروسات Anti-virus software
- التحكم بالدخول Access Control
- مضاعفة أنظمة التحقق من المستخدم Two-factor authentication systems.
- التدريب الجيد للموظفين Well-trained employees

قال تعالى : **وَلَا تَجْسُرُوا** ، **وَلَا يَقْتَبِ بِعُضْلِكُمْ بَعْضًا** .. الآية ١٢ الحجرات

و أعلم أعي العزة ان العلم امانت وستسال عنه يوم القيامة ،

قال تعالى: " إنا عرضنا الأمانت على السماوات والأرض والجبال فأبين أن يحملنها واشفقن منها وحملها الإنسان إنه كان ظلوما جهولا " الأحزاب آية ٧٢

فلا تغتر بعلمك وتستخدم هذه الأمانت في اذى الناس ، كن متواضعا واعلم ان الله سبحانه وتعالى قادر ان يسلب منك هذا العلم ويعطيه لغيرك ليفيد به الناس .

واعلم ان ديننا اكنيفه حذر بعدم الإضرار بالناس إن كان في ارزاقهم او في علمهم او في أنشطتهم ولا تكن من ذوى النفوس الضعيفة فهم جاهلون بان الله هو الرقيب وإنه سبحانه وتعالى ليس بظلام للعبيد .

فيمكنك ان تكون هاكل بل وكراكر ولكن في سبيل الله ، ما بالك اذا استخدمت كل ما لديك من علم و فنون وتقنية في خلق المطاوع الإباحية وتتبع اسرار العدو وصد الهجوم والإغترافات من قبل العدو

اليس ذلك في سبيل الله.

## الفصل الخامس

### التخلص من الفيروسات وملفات التجسس

#### الفيروس

هو برنامج صغير غالباً يكون غير مرئي يربط نفسه ببرنامج آخر ليتمكن من التكاثر و التكرار و الانتشار من خلال هذا البرنامج فعند تنفيذ هذا البرنامج المصاب بالفيروس ينتقل الفيروس إلى الذاكرة للجهاز المرسل إليه الفيروس و يستقر فيها و يصيب كل برنامج يتم تحميله في الذاكرة بعد ذلك قبل إعادة تحميله و قد ينشط الفيروس في يوم معين كما حدث مع فيروس تشرنوبل في ٢٤ أبريل أو عند نسخ برنامج معين أو عند تنفيذ برنامج عدد من المرات أو بعد عدة مرات من إعادة التحميل و هناك فيروسات تصيب الملفات و أخرى تصيب الجزء الخاص بتحميل الجهاز و الموجود في الاسطوانة الصلبة أو الاسطوانة المرنة.

قد يؤدي الإصابة بالفيروس الى تعطيل عمل البرامج او تقليل سرعته او اصابة الجزء الخاص بتشغيل جهاز الكمبيوتر مما يؤدي الى ايقاف عمل الجهاز او قد يؤدي الفيروس الى مسح منطقة جدول التقسيم- جدول التقسيم هو فهرس يحتوى على اسماء الملفات و اماكن وجودها على القرص الصلب .



تستهدف الفيروسات:

١- البرامج التنفيذية مثل:

.com, .exe, .ovl, .drv, .sys, .bin, .vbx, .dll

٢- البرامج التحميلية مثل:

Boot Record, Master Boot, FAT, PartitionTable

٣- متعددة الأهداف (البرامج التنفيذية والتحميلية)

كيف يمكن اكتشاف وجود فيروس على الحاسب الشخصي

تواترت في الآونة الأخيرة تحذيرات كثيرة بشأن إنتشار فيروسات الحاسب بحيث صار من السهل أن ينسب المرء أي إضطراب مريب يطرأ على أداء حاسبه الشخصي إلى احتمال إصابته بفيروس. ولكن الفيروسات في حقيقة الأمر لا تكون مسؤولة في بعض الأحيان عن أي إضطراب أداء الكمبيوتر، حيث إن بعض هذه المشكلات يكون ناجماً عن أسباب أخرى.

وربما يفاجأ المستخدم عند فتح مستعرض الإنترنت بوجود موقع إباحي على شاشة الكمبيوتر بدلاً من صفحة البدء الأصلية ويفترض أن

السبب في ذلك هو وجود فيروس ولكنه لا يكتشف وجود أي مشكلة عند تشغيل برنامج مكافحة الفيروسات ويتساءل عما إذا كان السبب في هذه المشكلة هو وجود فيروس. ويرجح أن يكون السبب وراء هذه المشكلة هو قيام موقع من المواقع التي زارها المستخدم "بختطف" مستعرض الإنترنت الخاص بالحاسب. فأحيانا ما يتلقى المستخدم رسائل يريد إليكتروني تحتوي على عناوين مواقع إليكترونية تبدو مشروعة، ولكن هذه المواقع في حقيقة الأمر تدخل تعديلات على مواصفات صفحة البدء.

وأحيانا ما يتلقى المستخدم رسائل تحذيرية بشأن تغيير مواصفات الصفحة ولكنه لا يعرف في بعض الأوقات كيفية التعامل مع هذه التحذيرات ويبادر بالضغط على مفتاح الموافقة. ولا تمثل هذه التغييرات من الناحية الفنية فيروسات ولكنها بلا شك تثير إزعاج المستخدم. ويتعين من أجل استرجاع المواصفات الأصلية لصفحة البدء فتح مستعرض الإنترنت واختيار قائمة أدوات ومنها إلى قائمة خيارات الإنترنت ثم يتوجب إلغاء عنوان الموقع الاباحي المدون في الخانة المخصصة لتسجيل عنوان موقع البدء وكتابة إسم صفحة البدء الأصلية. وعادة ما تتسبب الفيروسات في بطء عمل الحاسب وعملية تحميل البرامج واختفاء بعض الملفات المسجلة على الكمبيوتر والحيلولة دون عمل البرامج بشكل منتظم أو منع عملها على الإطلاق.

ومن الضروري أن يعرف المستخدم أن هناك عوامل أخرى خلاف الفيروسات يمكن أن تكون سبباً في إضطراب أداء الكمبيوتر. ولهذا السبب تكمن الصعوبة في تحديد ما إذا كان الجهاز مصاباً بفيروس أم لا. تماماً حينما يختلف كثير من الأطباء في تشخيص مرض واحد للأسف. وأفضل الحلول لمعرفة ذلك تتمثل في استخدام نسخة مطورة من برنامج خاص بمكافحة الفيروسات من إنتاج شركة معروفة. وتستخدم بعض الفيروسات قائمة عناوين البريد الإلكتروني كي ترسل نفسها في صورة ملفات ملحقه إلى أجهزة كمبيوتر أخرى. ولهذا السبب يتعين على المستخدم الاحتفاظ بنسخة متطورة من برامج مكافحة الفيروسات ويقوم بتشغيلها بحيث تتولى فحص الرسائل الإلكترونية الواردة والصادرة بصورة تلقائية ومنع انتقال الملفات المصابة بفيروسات.

ويتعين على المستخدم عندما يتشكك في وجود فيروس بأحد الملفات على جهاز الكمبيوتر الخاص به أن يبادر بإرسال هذا الملف إلى أحد مختبرات فحص الفيروسات المنتشرة في مختلف أنحاء العالم ولها مواقع عديدة على شبكة الانترنت.

## أولاً : التخلص من الفيروسات :

يمكن الوقاية من الفيروس بتشغيل إحدى برامج الـ anti virus التي تعمل في بيئة Windows

و التي تظل موجودة في ذاكرة الحاسب و عند دخول الفيروس بأي طريقة فإنها تمنعه و ترسل رسالة تحذيرية لمستخدم الحاسب مثل برنامج

### Norton Anti Virus

هذا البرنامج يقوم بفحص الذاكرة و ملفات النظام و قطاعات التشغيل عند بدء تشغيل الجهاز به و يمكنك إستخدامه للبحث عن الفيروسات و إزالتها سواء كان على القرص الصلب أو المرن و يمكنك إستخدامه لفحص أى ديسك مرن قبل إستخدامه و هو لديه قائمة بها آلاف الفيروسات يقوم بالبحث عنها و إزالتها لاحظ كذلك أنه يجب تطوير update برامج الوقاية و الكشف عن الفيروسات باستمرار حتى تواكب ظهور الأنواع الجديدة من الفيروسات.

وإختيار برنامج الحماية "مضاد الفيروسات" الأنسب لك ولجهازك كما نعلم ، هناك العديد من البرامج التي يقول مبرمجوها أنها هي الأفضل و تستطيع القضاء على كل الفيروسات و حتى الفيروسات الغير معروفة .

لا تصدق كل ما يقال .. فقد أثبت التجارب العملية أن ٩٩% من البرامج التي تم تجربتها لم تستطع أن تحمي الأجهزة التي تم إصابتها بفيروسات تتراوح خطورتها بين خفيف الخطورة إلى خطير جداً. ومن أشهر مضادات الفيروسات **Anti-virus**

**Norton anti-virus**

**PC Cillin**

**KasperSky Antivirus**

**McAfee Virus scan**

**NOD32**

**Vcatch**

**التخلص من الفيروسات دون الحاجة الى برامج**

سوف يتم الكشف عن الفيروسات من خلال موقع **Symantec** المتخصص في هذا العمل والذي يقدم لنا برامج حماية المختلفة منها برنامج

**Norton Antivirus .**

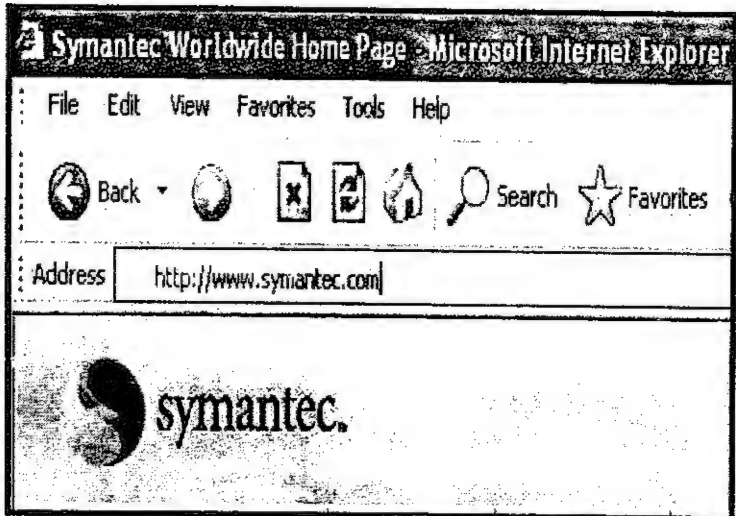
ويقدم لنا ايضا خدمة الكشف والتخلص من الفيروسات عن طريق الانترنت بدون حاجة الى البرنامج في جهازك.

ولكن هذا لا يعني أن تتخلي عن برامج الحماية ولكن هناك بعض الفيروسات التي


تغلق برامج الحماية ، فهذا واحد من الحلول للتخلص منها.

أولا قم بالدخول الى موقع **Symantec** الموجود على هذا العنوان:

**www.Symantec.com**



قم باختيار **security response**




[search](#)
[site index](#)

[日本](#)
[대한민국](#)
[台灣](#)
[中國](#)

[products and services](#)
[purchase](#)
[support](#)
[security response](#)
[downloads](#)
[about symantec](#)

# Global Security Solutions



## Security Response USA >

**Latest Threats**

- 06-21-04 Backdoor.Rackly.G
- 06-20-04 Backdoor.Racarmy.C

**Advisories**

- Microsoft DirectX DirectPlay Remote
- Malformed Packet Denial Of Service Vulnerability

**Downloads**

- Download Virus Definitions
- Download Security Updater
- Subscription Support
- Download Virus Removal Tool
- Symantec Security Check

## Announcements

**Continuing Professional Education Credits Available**

Symantec webcasts qualify CISSP/SSCP members for CPE credits. View our webcast offerings to register for security webcasts.


[more info](#)

**Spam Watch Response Center**

Protecting customers' privacy is a priority for Symantec. Visit the Spam Watch Response Center to learn more about suspicious email offers.

[more info](#)


## Enterprise Products and Services >



**Symantec Client Security**

Threat prevention through integrated antivirus, firewall and intrusion detection for remote, mobile, and networked client systems.

[more info](#)



**Norton AntiVirus 2004 Professional**

The world's most trusted antivirus solution with advanced protection.


[more info](#)

## Shop Home & Home Office >

© 1995 - 2004 Symantec Corporation. All rights reserved.

[license agreements](#) [legal notices](#) [privacy policy](#) [contact us](#)

بعد ذلك إبحث عن **check for security risk** واضغط عليها



**\$20**  
MAIL-IN  
REBATE

CLICK HERE

FREE Symantec® DeepSight™ Analyzer  
Norton Internet Security and Personal Firewall Users

CLICK HERE FOR FREE DOWNLOAD

### virus definitions

**Virus Definitions:**  
[Download Virus Definitions](#)  
[Online Virus and Security Check](#)  
[How do I update my definitions to the latest definitions?](#)  
[How do I purchase and activate my Definition Subscription?](#)  
[How do I download my definitions manually?](#)

### updates

**Security Updates:**  
[Symantec Enterprise Security Manager \(Jun 17\)](#)  
[Symantec Endpoint Alert \(May 3\)](#)  
[Symantec Definition \(May 13\)](#)  
[Symantec Internet Security \(Jun 4\)](#)  
[Symantec Security \(Jun 10\)](#)  
[Symantec Vulnerability Assessment \(Jun 15\)](#)  
[Symantec Host IDS \(May 3\)](#)  
[Symantec Incident Manager \(Feb 25\)](#)

### removal tools

[W32\\_Edget.B@mm](#)  
[W32\\_Kopra](#)  
[W32\\_Dont.Q](#)  
[Tool to reset shellopencommand registry keys](#)  
[W32\\_Sasser](#)  
[W32\\_Oasys@mm](#)

[View all removal tools ->](#)

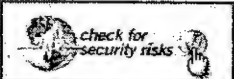
### am i protected?


**Intelligent Updater:**  
 Virus Definitions created June 21  
 Virus Definitions released June 21  
 Norton AntiVirus Corp. Edition:  
 Data Version: 60621af  
 Sequence Number: 32386  
 Extended Version: 6/21/2004 rev. 30  
 Total Viruses Detected: 67700

**LiveUpdate:**  
 Virus Definitions created June 19  
 Virus Definitions released June 19  
 Norton AntiVirus Corp. Edition:  
 Data Version: 60618e  
 Sequence Number: 32307  
 Extended Version: 6/19/2004 rev. 19  
 Total Viruses Detected: 67695

Norton AntiVirus for Mac Data released June 3

[Intelligent Updater vs. LiveUpdate: Click here for information.](#)






**symantec.**

**symantec security check**


**united states**

- [global sites](#)
- [products and services](#)
- [purchase](#)
- [support](#)
- [security response](#)
- [downloads](#)
- [about symantec](#)
- [search](#)
- [feedback](#)



**Symantec®  
Security Check**

Test your computer's exposure to online security threats  
and learn how to make your computer more secure.



© 1995-2004 Symantec Corporation.  
 All rights reserved.  
[Legal Notices](#)  
[Privacy Policy](#)



## قم بالضغط على Start الموجود تحت Virus Detection

Symantec

SECURITY INFORMATION   FREE SECURITY ALERT   SECURITY SOLUTIONS   HELP

### Symantec Security Check

Symantec Security Check tests your exposure to a wide range of online threats. It's free and efficient, and it helps you determine your Internet security needs.

#### Security Scan

IS YOUR COMPUTER SAFE FROM ONLINE THREATS?

[LEARN MORE](#)

#### Virus Detection

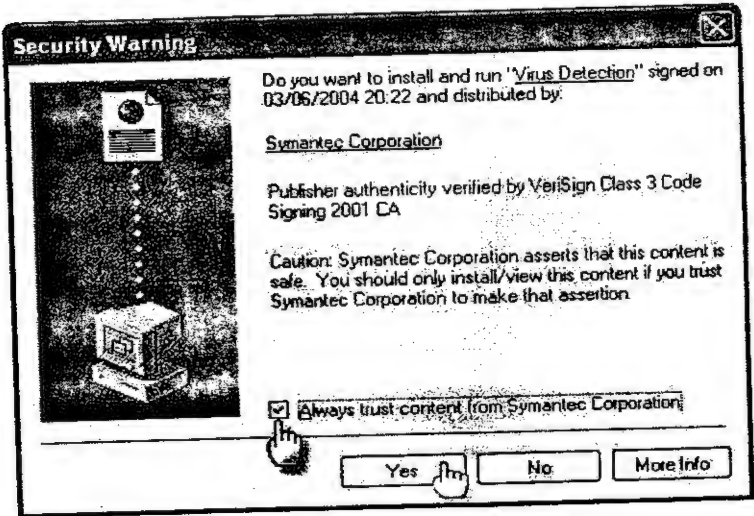
IS YOUR COMPUTER FREE OF VIRUSES?

[LEARN MORE](#)

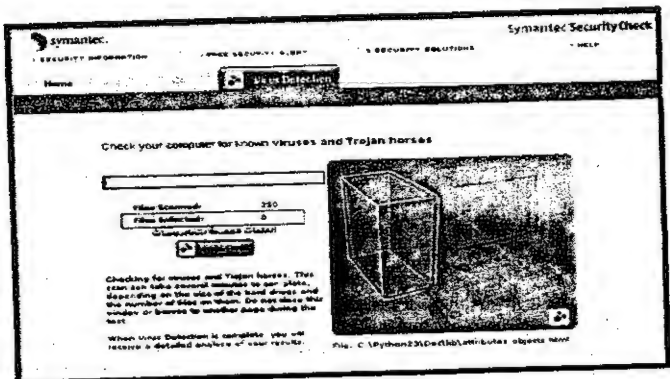
© 1995-2004 Symantec Corporation. All rights reserved. [Legal Notices](#) [Privacy Policy](#)

بعد ذلك سوف تظهر لك رسالة قم بالضغط على المربع لكي يظهر عليه

علامة ، واضغط **Yes**



سوف يبدأ الموقع بالبحث في جهازك عن الفيروسات وفي نهاية العمل  
سوف يظهر تقرير كامل عن حال جهازك ، فحاول أن تجرب هذه  
الطريقة الآن ..



## ثانياً إزالة ملفات التجسس

## Remove spy ware

١ - إختيار برنامج الحماية "مضاد ملفات التجسس" الأنسب لك و لجهازك لتنظيف جهازك من أى برامج تجسسية ، ويوجد العديد من البرامج التي تقوم بهذه المهمة ومن أهمها **Ad-Aware** و **Spy weeper** ، احرص على تحديث مضاد الفيروسات الخاص بك ، واستخدم برنامجاً غير معروف ( غير منتشر ) بصورة كبيرة لفحص جهازك من فترة لأخرى - يمكنك تثبيته على جهازك وعدم تشغيله الا في حالة الفحص فقط .

٢ - إختيار برنامج الحماية "مضاد الإختراقات أو الحائط الناري أو الجدار الناري الأنسب لك و لجهازك.

معظم البرامج المتخصصة بهذا المجال تفى بالغرض لكن لتعرف كل ما يحدث بجهازك وتمنع أي إتصال بين برامجك (التي قد تكون مضره أو مخله بأمن جهازك) و الإنترنت ، يمكنك إستعمال **Zone Alarm** :

ولنعلم جميعاً أن عملية التجسس قد تكون من مصنعي ومبرمجي برامج النظام والتصفح كما هو الحال في مايكرو سوفت التي تتجسس علينا

من خلال ويندوز .

٣- المتابعة لتحديثات البرامج التي تستخدمها في موقعك فمثلاً إن كنت تستخدم منتدى في موقعك ، فلا بد أن تتابع ولو بشكل شبه يومي آخر التحديثات التي ظهرت لهذا البرنامج وكذلك سد جميع الثغرات والترقية إلى آخر إصدار.

٤- حماية المجلدات المهمة بجدار ناري من خلال لوحة التحكم الخاصة بموقعك ولو على سبيل المثال **cPanel** فلتقم بحماية المجلدات المهمة مثل المجلد **admin** للمنتدى ، حتى إذا ماتم إختراق الموقع لا قدر الله ، فلن يستطيع المخترق الدخول للوحة التحكم إلا بعد تخمين كلمة السر الثانية

٥- عدم إستخدام التصريح ٧٧٧ إلا عند الضرورة القصوى ويجب عليك أن تقوم بحماية المجلد أيضاً بجدار ناري حتى تضمن عدم وجود تلاعب ، كذلك إن كنت تستخدم برنامج لرفع الملفات فعليك إبطال تحميل الملفات المؤثرة مثل

ملفات **.php .php3 .phtml .pl .cgi** ، وذلك من خلال الملف **htaccess** لحماية موقعك.

٦- لا تعطي صلاحيات الدخول إلى لوحات التحكم في موقعك إلا  
لشخص تثق فيه ١٠٠ %

ومع كل هذه الإحتياطات لا يوجد شئ اسمه حماية ١٠٠ % ولكن  
نسعى لإغلاق كل السبل لتخريب مواقعنا من قبل الكراكرز .

يقول الله تعالى: " **ولا تجسسوا** ولا يغتب بعضكم بعضا أيحب أحدكم  
أن يأكل لحم أخيه ميتا فكرهتموه واتقوا الله إن الله تواب رحيم "  
سورة الحجرات الآية ١٢

## الفصل السادس

### الحفاظ على البريد الإلكتروني من الاختراق

١. يجب أن تكون كلمة المرور (كلمة السر) **pass word** طويلة وتحتوي على حروف وأرقام ورموز مثال **sc2004x**
٢. أن تكون كلمة السر عشوائية وغير مرتبة ومسلسلة ،
٣. لا تكتب الأسماء أو تاريخ الميلاد أو أسماء الأولاد أو رقم الهاتف أو المدينة.
٤. لا تكشف عن معلومات خاصة لأي شخص تقوم بمراسلته عبر البريد الإلكتروني
٥. لا تجعل اسم المستخدم **user name** نفسه كلمة المرور أو حتى أن تضيف إليها بعض الحروف أو الأرقام مثال:  
**User name : khaledmk**  
**Pass word : khaledmk2000**
- هذا خطأ كبير يسهل على المخترق معرفة كلمة السر خصوصاً أن هناك برامج تقوم بتخمين كلمات السر.
٦. حاول أن تجعل لكل بريد كلمة مرور خاصة به إن كان لك أكثر من بريد إلكتروني
٧. إن كنت سريع النسيان فاكتب كلمة السر في ورقة أو حتى في

ملف بجهازك بشرط أن تقوم بعملية تمويه لكلمة المرور ، فمثلاً إن كانت كلمة المرور الخاصة بك هي **egypt2000** مثلاً فاكتبها في مذكرتك بأن تضيف حروف أو أرقام زائدة للتمويه فمثلاً يمكنك كتابتها **kmkegypt2000** أو **egypt2000yes** ، وبالطبع أن فقط تعلم أن هذه الإضافة مجرد تمويه للكلمة الحقيقية وهي **egypt2000** بهذه الطريقة يمكنك حفظ كافة كلمات المرور في ملف بالإنترنت أو في ورقة.

٨. أن يكون لك بريد خاص لإستخدامه في المنتديات والقوائم البريدية و الماسنجر

٩. أن تقوم بتغيير كلمة السر كل فترة للتأكد من أنك في أمان ممن قد يكونوا بالفعل يستغلون كلمة السر فقط لفتح رسائلهم والإطلاع على أسرارهم وأعمالهم دون أن تدري.

١٠. لا تدخل لبريدك إلا من موقعه الأصلي حتى لا تقع في الفخ

١١. عند الإنتهاء من قراءة وتصفح رسائلهم إضغط على أيقونة الخروج **log out** أو **exit** لغلص صندوق البريد.

١٢. لا تقوم بفتح ملفات مرفقة تأتي إليك من بريد **e-mail** مجهول وأنصح أن لا تفتح مطلقاً أى بريد لا تعرف مصدره.

١٣. إرسال رسالة فوراً للمدعم خدمة البريد إن كانت مجاناً مثال ياهو بأن بريدك قد سرق .

١٤. حاول أن تقوم بتفريغ صندوق البريد ووضع (حفظ) ملفاتك ورسائلك الواردة إليك داخل ملف بجهازك ويستحسن في قرص مرن أو CD ثم قم بحذف جميع رسائلك من بريدك الإلكتروني ، قم بهذه الطريق كل فترة ..

١٥. لا تجعل اسم المرور مخزن (remember pass word) في الجهاز ، أى لا تجعل اسم المرور يأتى إليك تلقائياً (الإكمال التلقائى auto complete) بمجرد كتابة اسم المستخدم كما يفعل بعض المستخدمين ، فهذا يعطى فرصة للمخترقين للوصول إلى كلمة السر بسهولة ، ولتعطيل هذه الخاصية إتبع ما يلى من إكسيلورر :

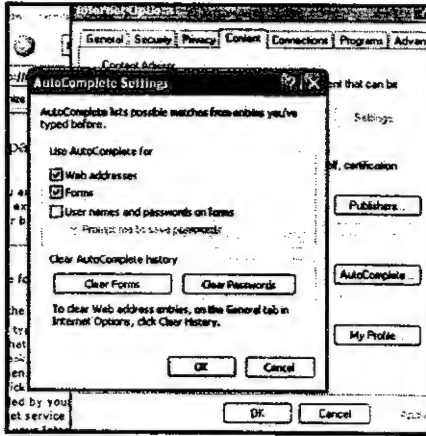
**Tools**

**Internet options**

**Content**

**Auto complete**





User names and pass words on forms: (remove the sign)

Press ok

عند دخولك بعد ذلك الموقع لكتابة إسم المستخدم وكلمة السر ستأتي نافذة أو تجدها تحت نافذة كلمة المرور : هل تريد الإكمال التلقائي أو هل تريد حفظ كلمة المرور ، بالطبع اختر لا .

## الفصل السابع

### تأمين الدفع الإلكتروني

#### أمن الإنترنت

لقد فرضت شبكة الإنترنت علينا بل و أصبحت أحد مستلزمات الحياة اليومية . فهي توفر وسيلة للدخول إلى كم هائل من المعلومات، وتضعها في حوزتنا بكل سهولة. وأهم من ذلك، أنها باتت تلعب دوراً هاماً في أعظم إبداعات و إختراعات القرن العشرين والواحد وعشرون وهي التجارة الإلكترونية أو e-Commerce.

فإلى جانب إمكانية الإنترنت بوضع كميات غير محدودة من المعلومات بين أيدينا، هناك إمكانية شراء المنتجات والخدمات دون مغادرة المنزل، فالتجارة الإلكترونية تعني كل معاملات البيع والشراء وتبادل المعلومات ، أى أنه بمقدورنا القيام بشراء الكتب، وأجهزة الكمبيوتر، وتذاكر السفر، والسيارات، وغيرها في أي لحظة.

ومع أن هذه الفكرة كانت مشجعة في بادئ الأمر، إلا أن إنتشارها كان بطيئاً نسبياً بسبب مخاوف العامة، فحفظ المعلومات المصرفية وبيانات بطاقات الائتمان في مكان مجهول يعد مخاطرة كبيرة. ومع أن هذا الخطر محدود، إلا أنه لايزال موجوداً.

لهذا الخطر علاقة كبيرة بحقيقة أن معلومات بطاقات الائتمان ترسل ضمن نص غير مشفر، وهذا يعني أنه يمكن سرقة هذه المعطيات واستخدامها بهدف الإحتيال. لقد تم تطوير تقنيات مختلفة للتغلب على هذه المشكلة وحماية المستهلك، مما زرع الثقة في نفوس الناس وشجعهم على الشراء عبر الإنترنت.

فكان ظهور بروتوكول S-HTTP هو نسخة أمنية من بروتوكول HTTP ويُستخدم للإتصال مع مواقع الويب. إن أحد مزايا بروتوكول S-HTTP هو أنه ليس بروتوكولاً خاصاً، الأمر الذي ساعد على إنتشاره في غالبية برمجيات خادمت الويب، ومع ذلك فإن دعم برامج المتصفحات لهذا البروتوكول لا يزال محدوداً.

وقد أنتجت شركة Netscape بروتوكولاً منافساً يدعى SSL وقالت الشركة أنها ستقوم بدعم بروتوكول S-HTTP ضمن برامجها في المستقبل القريب.

إذاً بإمكان المستخدمين التعامل مع كلا البروتوكولين، والإتصال بالخادمت التي تستعمل HTTP أو SSL.

**هناك** أنواع كثيرة يمكنك منها معرفة إذا كان الموقع الذى تعمل من خلاله أو تحول نقوداً من خلاله آمناً بتلك البروتوكولين أم لا :

## المثال الأول : حرف الـ S بجوار http

هو دليل على أن هذا الموقع محمي بروتوكول https

وحرف s يرمز إلى أن الموقع مؤمن secure

### Secure Hypertext Transfer Protocol

وهو بروتوكول النقل الآمن لنصوص الانترنت

وكما ذكرنا سابقاً إن بروتوكول S-HTTP هو نسخة أمنية من

بروتوكول HTTP ويُستخدم للاتصال مع مواقع الويب.

يعمل بروتوكول S-HTTP بين طبقة TCP/IP وبروتوكول

HTTP. فعندما يطلب بروتوكول HTTP إرسال معلومات إلى مخدّم

آخر، يقوم بإرسال الطلب إلى بروتوكول S-HTTP ليتحقق من أن

المعلومات مشفرة وصحيحة قبل إرسالها إلى بروتوكول TCP/IP ليقوم

بنقلها.

فمثلاً : إذا أردت أن تدخل على موقع مثل paypal وتقوم

بتسجيل اسم المستخدم وكلمة السر فلا بد أن تتأكد أن http://

تحتوى على حرف s أى لابد أن يظهر الموقع بشريط العنوان بهذا

الشكل

<https://www.paypal.com>

حرف S بجوار https://

https://www.paypal.com/

Sign Up | Log In | Help

Welcome Send Money Request Money Merchant Services Auction Tools

Member Log-In Secure Log In

Registered users log in here. Be sure to protect your password.

Email Address:

[Forgot your email address?](#)

Password:

[Forgot your password?](#)

New users [sign up here!](#) It only takes a minute.

Internet

هذا شكل القفل أيضاً بموقع paypal

ومن هنا أنت قد لاحظت أن http:// بها حرف s لتكون https://  
فكثير من الرسائل المغرضة للإختراق قد تأتي إليك مثلاً بأن تقوم بعملية  
تأكيد معلوماتك في خلال ساعات وإلا سوف يعلق موقعك  
suspended ويعطيك لينك لكي تضغط عليه لتقوم بعملية

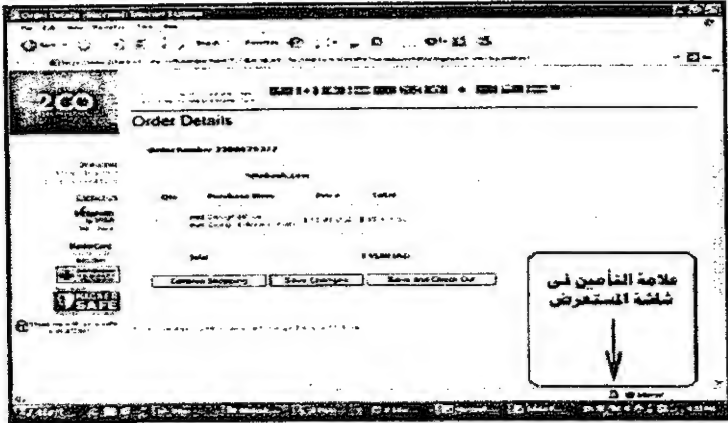
التسجيل فتقع في الفخ وتقع فريسة للكراكرز عديمي الضمير والإخلاق ، لذلك إذا قمت بالضغط على هذا اللينك فتأكد أن الموقع الذى سيظهر لك به حرف S مثال <https://> وإن لم يظهر لك هذا الحرف فتأكد مائة في المائة أنه فخ ..

ولكن الأصوب أخى المستخدم أن لا تدخل أبداً إلى موقع بالإنترنت من خلال رسالة إيميل E-mail .

### المثال الثانى : وجود شكل القفل بالشريط الأسفل

هو دليل على أن هذا الموقع محمى ببروتوكول SSL للتأكد من تأمين عملية الشراء الإلكتروني باستخدام البطاقة الائتمانية عبر الانترنت فى أى موقع قم بإجراء الخطوات التالية:

- عند الضغط على زر الشراء سيتم فتح موقع شاشة الدفع باستخدام البطاقة الائتمانية مثال موقع **2checkout** أو موقع **stormpay** أو **e-gold** أو حتى موقع **paypal** إن كنت من قاطنى الدول المدرجة لها، ستظهر شاشة الشراء وإدخال البيانات كما بالشكل التالى.
- بالنظر إلى الشريط السفلى الموجود فى نافذة برنامج المستعرض (انترنت اكسبلورر) على سبيل المثال.



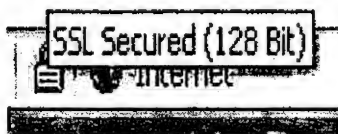
- سوف ترى قفل ذهبي صغير في الشريط ، وهذا الشريط يدل على أن هذا الموقع مؤمن للشراء ويحتوي على بروتوكول سرية البيانات **SSL** كما بالشكل



قم بالوقوف بمؤشر الماوس فوق القفل مباشرة فيظهر لك مربع أصفر صغير فوق القفل يشير إلى بروتوكول التشفير المستخدم . (و من المعروف أن بروتوكول التشفير المستخدم في تأمين البيانات على مواقع الويب هو :

بروتوكول طبقة التأمين **SSL** أو **Secure Socket Layer** أما

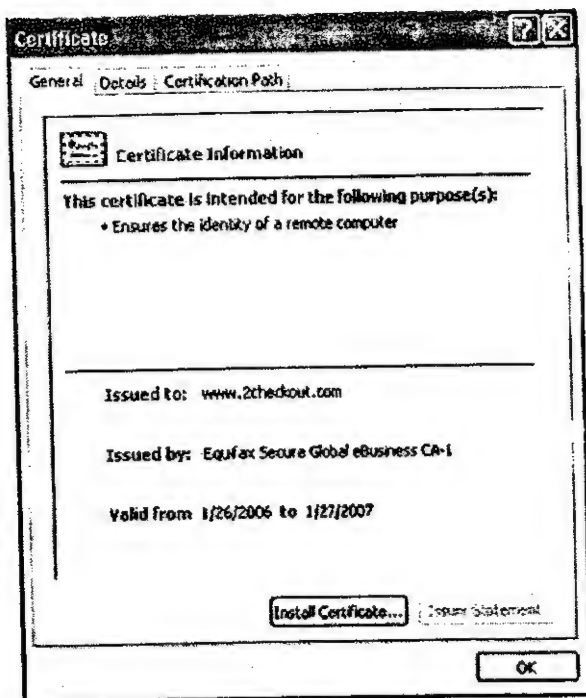
الرقم ١٢٨ فهو عدد الـ **bits** المستخدمة في التشفير وهو رقم عالٍ في عملية التأمين.



بهذا تكون قد تأكدت من تأمين عملية البيع الإلكتروني في أي موقع للبيع الإلكتروني.

ولزيادة التأكد من أن شهادة التأمين صادرة فعلياً للجهة التي تمنحها بيانات بطاقتك الائتمانية، يمكنك الضغط بمؤشر الماوس مرتين متتاليتين على القفل الذهبي نفسه ليتم فتح نافذة مربع صغير به بيانات شهادة التأمين (يرجى قراءة السطر الخاص بإصدار الشهادة) ومطابقته بإسم مانح خدمة الشراء الإلكتروني مثال **2Checkout** أو خدمة تقوم باستلام النقود أون لاين **Online** كما بالشكل :





ملحوظة :

بروتوكول SSL

يقوم بروتوكول SSL بإنشاء طبقة إرسال خاصة بدلاً من استخدام

بروتوكول HTTP ، مما يعني أن بمقدور النظام العمل مع أي من بروتوكولات الإنترنت، بما في ذلك HTTP و FTP و Telnet و Gopher يعمل بروتوكول SSL من خلال تأسيس قناة اتصال آمنة ومنفصلة لكافة الرسائل التي تستخدم بروتوكول HTTP ويتم إعداد هذه القناة الآمنة على المخدم وعلى المتصفح بواسطة برمجيات SSL خاصة.

## بروتوكول الحركات المالية الآمنة SET

طوّرت مجموعة من الشركات العالمية الرائدة (منها مايكروسوفت، وآي بي إم (IBM)، وفيزا (VISA)، وماستر كارد (MasterCard)) بروتوكولاً لعمليات الدفع (payment protocol)، أطلقت عليه اسم بروتوكول الحركات المالية الآمنة (Secure Electronic Transactions - SET). والغاية من هذا البروتوكول ضمان الحفاظ على أمن البيانات (خصوصيتها وسلامتها (integrity) والتحقق من وصولها إلى الجهة المطلوبة) أثناء إجراء الحركات المالية (Financial transactions) عبر شبكة مفتوحة مثل الإنترنت. ويشبه هذا البروتوكول - إلى حد كبير - بروتوكول الطبقات الأمنية (Secure Socket Layers- SSL) في إسناده إلى التشفير والتواقيع الرقمية .

وللحفاظ على خصوصية وسلامة المعلومات المنقولة عبر الإنترنت بين الزبائن وهم حاملو بطاقات الإئتمان (cardholders) والتجار (Merchants)، يستخدم بروتوكول الحركات المالية الآمنة (SET) برمجيات تُدعى برمجيات المحفظة الإلكترونية (electronic wallet software). وتحوي المحفظة الإلكترونية رقم حامل البطاقة (cardholder number)

والشهادة الرقمية (digital certificate) التابعة له، أما التاجر، فتكون له شهادة رقمية صادرة عن أحد البنوك المعتمدة. ويستخدم كل من حامل البطاقة والتاجر الشهادة الرقمية التابعة له، مما يتيح لكل منهما التحقق من هوية الآخر عند إجراء الحركات المالية عبر الإنترنت.

وإلى جانب شركتي فيزا وماستر كارد ، هناك حالياً العديد من الشركات العالمية التي تدعم هذا البروتوكول ، ومنها :

مايكروسوفت Microsoft ،

نتسكيب Netscape



فيرى ساين (Verisign)

(Systems Teresa).

## عملية الشراء وفقاً لبروتوكول الحركات المالية الآمنة (SET)

تتضمن عملية الشراء وفقاً لبروتوكول الحركات المالية الآمنة (SET) خمسة أطراف أساسية هي:

١. حامل البطاقة الائتمانية (cardholder) - وهو الزبون
  ٢. موفر المحفظة الإلكترونية (electronic wallet provider)
  ٣. التاجر (Merchant)
  ٤. معالج عمليات الدفع (acquirer or payment processor)
  ٥. بوابة الدفع (payment gateway).
- وحامل البطاقة (cardholder) هو شخص لديه حساب بطاقة ائتمانية (لدى فيزا أو ماستر كارد). ويستخدم هذا الشخص محفظة إلكترونية تحوي شهادات رقمية لبروتوكول الحركات المالية الآمنة (SET). وحامل البطاقة هو الزبون (customer) في هذه العملية.
- موفر المحفظة الإلكترونية (electronic wallet)

(provider) فهو المؤسسة المالية التي تزود الزبائن بالأدوات التي تُتيح - بشكل آمن - شراء البضائع والخدمات عبر الإنترنت. ومن هذه الأدوات الشهادات الرقمية، أو شهادات بروتوكول الحركات المالية الآمنة (SET certificates).

التجار (merchants) فهم الشركات والأفراد الذين يعرضون البضائع والخدمات عبر الإنترنت. وكما يتمكن هؤلاء التجار من التجاوب مع الحركات المالية التي يقوم بها الزبائن، لا بُدَّ لهم من الإرتباط بعلاقة مع معالجي عمليات الدفع (payment processors) أو مؤسسات مالية معتمدة أخرى.

معالج عمليات الدفع (acquirer or payment processor) وهو المؤسسة المالية التي تزود التجار بالحسابات (accounts)، وتتولى التحقق من عمليات الدفع التي قام بها الزبائن، بالإضافة إلى التعامل معها ومعالجتها.

بوابة الدفع (payment gateway) هي الجهاز الذي يشغله معالج عمليات الدفع (acquirer). ويتولى هذا الجهاز معالجة رسائل الدفع التي يتلقاها من التجار، وأوامر الدفع التي يتلقاها من حاملي البطاقات.

# إجراء الحركات المالية وفقاً لبروتوكول الحركات

## المالية الآمنة SET

يقوم الزبون في أول الأمر بفتح حساب بطاقة ائتمانية (credit card account) (ماستر كارد (MasterCard) أو فيزا (VISA)) في أحد البنوك، ثم يُصدر البنك إلى صاحب البطاقة برنامجاً خاصاً ببروتوكول الحركات المالية الآمنة (SET) يُدعى برنامج المحفظة الإلكترونية. وتُستخدم هذه المحفظة في الشراء وإجراء الحركات المالية عبر الإنترنت. وتُثبت المحفظة الإلكترونية في كمبيوتر المستخدم، حيث يُمكن له الدخول إليها في أي وقت للقيام بعملية الدفع عبر الإنترنت. وتحتوي هذه المحفظة معلومات مثل رقم البطاقة الائتمانية (credit card number)، وشهادة بروتوكول الحركات المالية الآمنة (SET certificate)، وتاريخ إنتهاء البطاقة، إضافة إلى معلومات أخرى. ويمكن تنزيل برنامج المحفظة من الإنترنت، ويكون هذا البرنامج مؤمناً بكلمة مرور pass word. ومن جهة أخرى، تُعدّ شهادة بروتوكول الحركات المالية الآمنة (SET certificate) دليلاً على أن البنك قد تَحَقَّق من هوية حامل البطاقة. وللحصول على هذه الشهادة، يُحوّل الزبون إلى جهة مخوَّلة بمنح الشهادات ومعتمدة لدى البنك. ويفتح التاجر حساباً لدى معالج عمليات الدفع (payment

processor) الذي يختاره (قد يكون بنكاً)؛ ليحصل على ما يلزمه من برمجيات لإستخدام بروتوكول الحركات المالية الآمنة. وتتضمن هذه البرمجيات شهادة بروتوكول الحركات المالية الآمنة (SET certificate) الممنوحة للتاجر، والمفتاح العام (public key) لمعالج عمليات الدفع المختار. وتستخدم هذه البرمجيات لمعالجة الحركات المالية على الإنترنت.



واللحصول على اى معلومت تخص برامج اُكمايت وُحْميلها وُحْدبثها  
مجاناً برجاء زيارة موقعنا على الإنترنت

**[www.books4internet.com](http://www.books4internet.com)**

أو زيارة المنتدى مباشرة

**[www.books4internet.com/vb](http://www.books4internet.com/vb)**

كل ما عليك فعله أن تقوم بتسجيل بريدك الإلكتروني

واسم المستخدم وكلمة السر للدخول

بعدها

يمكنك الدخول رقم بإرسال أية أسئلة خاصة

بالتجارة الإلكترونية و امن المعلومات

أو أى موضوع خاص بالكمبيوتر والإنترنت

وتكنولوجيا المعلومات

المشرفين على المنتدى مهندسون متخصصون

الآن إذهب إلى موقعنا

**[www.books4internet.com](http://www.books4internet.com)**

لترى أيضاً العروض والخصومات الخاصة بكتب المركز

وأيضاً يمكنك التسجيل لحضور ندوات مجانية عن التجارة الإلكترونية.

## الفصل الثامن

### طرق امن المعلومات واكفاز على البيانات

#### ١ - طريقة لوضع كلمات سرية لملفات الوورد

تستطيع ذلك وبدون استخدام أي برنامج .. فمثلا لا يوجد من لا يستخدم برنامج وورد تبع الأوفيس .. أغلبنا نستخدمه هذا إذا لم يكن الجميع .. فبعملك على برنامج وورد سوف تحتاج بالتأكيد في بعض الأحيان إلى توفير بعض الخصوصية لمنع الآخرين من معرفة أسرارك الشخصية أو أسرار عملك .. فهذا هو الحل :

أولاً : عليك أن تفتح المستند الذي تريد أن تضع له كلمة سر والذي تريد أن تمنع الآخرين من الإطلاع عليه أو عملية تخريب..

ثانياً : من القائمة الرئيسية أضغط على ملف ( File )

ثم اختر حفظ في.. ( Save As )

ثالثاً : سوف تفتح لك نافذة الحفظ لا تحفظ الآن انتظر .. من خلال

صفحة الحفظ ابحث عن كلمة أدوات ( Tools )

وسوف تجدها في الأعلى .. أضرب على لسان التبويب بتاعها وعندها

سوف ينسدل لك لسانه اختر الآن ( General Option )

رابعاً : سوف تفتح لك نافذة .. أنظر إلى الأسفل سوف تجد مستطيلين

**( Password to open )** الأول بعنوان

وهنا ضع كلمة السر التي تريدها .. والمستطيل الآخر بعنوان

**( Password to modify )**

**( OK )** وهنا كرر كلمة السر السابقة .. ثم اضغط على زر موافق..

خامساً : بعد ضغطك زر **( OK )**

سوف يظهر لك مربع آخر بنفس عنوان المستطيل الأول السابق الذكر

ما عليك سوى كتابة كلمتك السرية السابقة ،، ثم اضغط **( OK )**

.. أيضاً سوف يظهر لك مربع آخر بنفس عنوان المستطيل الثاني

السابق الذكر ،، ما عليك سوى تكرير كلمتك السرية ،، ثم اضغط

على **OK**

سادساً : الآن اختر المكان الذي تريد أن تحفظ مستندك فيه ،، ثم

اضغط على زر .. حفظ **( Save )**

.. وبهذا تكون قد حفظت الملف المحمي بكلمة سر..

**ثانياً : طريقة لإخفاء ال IP الخاص بجهازك**

وذلك حتي تتجنب أخطار الهاكرز والمحترفين وتكون في أمان ولكن هذا

الأمان من اختراق الجهاز وليس الفيروسات .

لذلك لابد من وضع برامج حماية ممتازة جدا بحيث يصعب اختراقها  
ولتفيذها :

انقر **Click** شمال علي **Start** ثم اختر بالنقر **Click** شمال علي  
**Run** ثم اكتب **Cmd**

ثم اضغط علي **Enter** سوف تفتح واجهة الدوس  
ثم اكتب **drwatson** في الواجهة المفتوحة ثم اضغط علي مفتاح  
**Enter** من لوحة المفاتيح سوف يتم إخفاء **IP** الخاص بالجهاز فورا  
ويظهر مربع حوار يخبر بذلك أنك أتركة مفتوح  
بالطبع رقم الـ **IP** لا يختفى بالنسبة لك أنت ولكن هذا الرقم يختفى  
لأى مخترق آخر ..

## وللحفاظ على البيانات

البيانات المخزنة على الحاسبات هي أغلي ما يوجد داخل وحدات  
التخزين و هي أكثر أهمية من البرامج و التطبيقات مهما كانت قيمتها،  
لأن فقدانها يعني عدم إمكانية إستعادة هذه الملفات مرة أخرى، و قد  
تزداد المشكلة أكثر إذا لم يكن في استطاعتنا إدخال البيانات للحاسب  
مرة ثانية من النسخة الورقية.

و على الرغم من أن التقنية الحديثة المستخدمة في صناعة وحدات  
التخزين الرئيسية **Hard Disk** تطورت تطورا كبيرا بحيث

أصبحت تلك الوحدات تعيش لفترات أطول كما صارت سعتها التخزينية أكبر و زادت سرعتها بدرجة كبيرة إلا أن معدلات حوادث فقد البيانات لا تزال في إزدیاد . و تعتبر أعطال وحدات التخزين الرئيسية التي تعتمد على تقنية السطح المغناطيسي في حفظ البيانات مسئولة عن نسبة كبيرة من هذه الحوادث و ذلك بالإضافة إلى الأخطاء البشرية من المستخدمين .

### أساليب الوقاية

و حتى لا تقع ضحية لفقد ملفاتك من على الحاسب الخاص بك يجب أن تراعي النقاط التالية :

١- وحدة التخزين الحديثة و التي أصبحت ذات سعة أكبر من وأحدث حيث صارت تخزن أعداداً هائلة من الملفات . فيقدر الخبراء أن سعة وحدات التخزين أصبحت أكبر ٥٠٠ ضعف عما كانت عليه منذ عشر سنوات . و كلما زاد عدد الملفات التي يتم الاحتفاظ بها على وحدة التخزين الواحدة كان ذلك يعني أن مشكلة تلف هذه الوحدة ستصبح أخطر لأنها تحتوي على آلاف الملفات .

و إذا حدث إنقطاع مفاجئ للتيار الكهربائي أثناء تحرك رأس القراءة و الكتابة على السطح المغناطيسي للوحدة فإن ذلك قد يسبب إحتكاكاً شديداً بين رأس القراءة و الكتابة و السطح الحساس للوحدة مما قد

يتسبب في تلفها.

٢- الاختراعات الحديثة جعلت الإنسان يقوم بتخزين معلومات و بيانات أكثر على الحاسبات الإلكترونية فوسائل إدخال البيانات للحاسب تنوعت ف بجانب لوحة المفاتيح التي يمكنها إدخال الحروف و الأرقام يمكننا أن نستخدم الماسح الضوئي لإدخال الصور و المستندات و نستخدم الكاميرات الرقمية **digital camera** و كاميرات الفيديو لإدخال الصور و الأفلام . كما أصبحت شبكة الإنترنت مصدراً جديداً للمعلومات التي يمكن تخزينها على الحاسب .

و بصفة عامة فإن الاعتماد الكبير على تخزين مختلف أنواع البيانات على الحاسبات الإلكترونية وضع بعداً جديداً لحوادث فقد البيانات نتيجة لعيوب تصنيع و استخدام وحدات التخزين أو للأخطاء البشرية حيث صار حجم المعلومات التي يمكن أن نفقدها كبيراً بشكل مؤثر نظراً لاعتمادنا على الحاسبات في تخزين كل المعلومات التي نتعامل معها و لذا فإن فقد هذه البيانات أو عدم التمكن من الوصول إليها يعني أن قطاعات مهمة من المجتمع يمكن أن تتوقف عن العمل نتيجة لحوادث فقد البيانات.

٣- استخراج نسخة احتياطية **Backup** من الملفات هي الطريقة الوحيدة التي يمكننا أن نعالج بها مشاكل فقد البيانات، و لكن للأسف أن التقنية الحديثة المستخدمة في الحصول على النسخ الاحتياطية لم

تستطع أن تقدم الحل الشافي لهذه النوعية من المشاكل و ذلك رغم الجهود الكبيرة التي بذلت في هذا المجال فكثير من المستخدمين يكتشفون عند تعرضهم لفقد البيانات أن النسخ الاحتياطية التي يحتفظون بها قد أصبحت عديمة الفائدة نظراً لأنها غير كاملة أو غير حديثة أو تم استخراجها بطريقة خطأ و لم نعرف بهذا العيب إلا عندما وقعت المشكلة و حاولنا إعادة الملفات المفقودة.

## الفصل التاسع

### الثغرات

هناك ثغرات وطرق كثيرة تمنع حتى المواقع التي تكشف الثغرات المفتوحة في جهاز الضحية من كشفها لأنه حتى تلك المواقع تعتمد على قاعدة بيانات تحتوي على معلومات محدده لديها .

فهنا ما زالت المشكلة تتفاقم ، حيث ضعفاء النفوس الذين يدعون أنفسهم بالهاكرز إستدلوا ويستدلون على طرق عديدة تعتمد على ثغرات أنظمة التشغيل من خلالها يصلون إلى المعلومات السرية مثال المعلومات الخاصة بتداول الأسهم والحسابات الشخصية وحسابات البنوك وأرقام بطاقات الإئتمان وغيرها.

وأحد أخطر الطرق المنتشرة عند الهاكرز هو إستخدام أحد ثغرات أنظمة تشغيل الكمبيوتر في إرسال برامج التجسس وغيرها من برامج أدوات الهاكرز ، طبعاً بعد تغيير بصمة برنامج التجسس المرسل لكي لا يكتشفه برنامج الحماية.

و من المعروف أنه إذا تركت جهاز الكمبيوتر متصل على الإنترنت لبضع ساعات سوف تجد ملف تجسس لأنه في أى لحظة قد يستقبل ملفات تجسس ، هذه الثغرة في نظام التشغيل تتيح للهاكرز إرسال برامج التجسس بطريقة عشوائية لأي كمبيوتر متصل بالإنترنت.



اولاً : ثغرات موجودة في ويندوز إكس بي window xp  
 هناك ثغرات في أجهزة الإكس بي و دائماً تكون مدخل للهacker  
 والكرakerز ومعظمنا لا يعرفها ولا كيف يمكن التخلص من هذه الثغرات  
 الموجودة في xp

### الثغرة الاولى :

تعتبر إحدى البوابات الخطيرة للفيروسات وملفات التجسس  
 وللتخلص من هذه الثغرة :

١- إذهب إلى لوحة التحكم panel control

٢- ثم خيارات المجلد folder options

٣- ثم أنواع الملفات file types

وهناك ستجد :

Windows script host setting file

قم بحذفه فوراً

### الثغرة الثانية :

وتسمى ( مشاركة ملفات بسيطة ) simple file sharing

ولكن تفعيلها ليس بسيطاً بل هو خطير جداً ..

إتبع الآتي :

١- من خيارات المجلد **folder options**

٢- ثم عرض **view**

٣- يجب إزالة علامة الصح من داخل المربع أمام :

مشاركة ملفات بسيطة ( ينصح بذلك ) .

(use simple file sharing) (recommended)

الثغرة الثالث :

وتسمى : ( عدم حفظ الصفحات المشفرة إلى القرص ) .

**save encrypted page to disk**

إتبع الآتى :

١- لوحة التحكم **control panel**

٢- خيارات انترنت **options internet**

٣- خيارات متقدمة **advanced**

٤- وضع علامة صح داخل المربع :

( عدم حفظ الصفحات المشفرة إلى القرص )

**don't save encrypted page to disk**

ثم موافق .

ثانياً : ثغرة أمنية خرجت في متصفح الإنترنت مايكروسوفت

**Microsoft Internet Explorer**

تم اكتشاف خطأ برمجي في متصفح الإنترنت لمايكروسوفت تمكن بعض المواقع من تثبيت مكونات جديدة للنظام إما ان تكون **ActiveX** او **dll** تستخدم لتنفيذ أمر برمجي.

### ثالثاً : ثغرة أمنية خطيرة Heap Overflow في متصفح الإنترنت لمايكروسوفت

الثغرة الأمنية في مكونات ويندوز **COM Object** تسمح بإنشاء صفحة إنترنت يستطيع من خلالها إنزال وتشغيل ملف تنفيذي في جهاز المستخدم  
الأنظمة المصابة

**Windows 2000 Server SP4 , Internet Explorer 6.0 SP1**  
**Internet Explorer 6.0 SP1 , Windows XP SP2**  
خطورة هذه الثغرة أنه لا يوجد أي تحديث أمني إلى الآن.

### ماذا بعد

هل شركات أنظمة التشغيل لا تدري أن هناك ثغرات في أنظمتها بالطبع هي تعلم ذلك بل و تصرح بين الحين والآخر بأنها قضت على ثغرات نظامها..

ولأننا جميعاً مؤمنين بأن هناك ثغرات كثيرة تسمح لضعفاء النفوس بالتطفل على خصوصياتنا ، ونعرف تماماً مدى سهولة حصول الهاكرز

على هذه البرامج . فهناك برامج هاكرز مختصة باستخدام ثغرات مايكروسوفت والبال توك والماسنجر والبرامج التي تحتاج للتحديث وغيرها .

فبمجرد استخدام برنامج مثل Super Scan أو غيره من البرامج وهي كثيرة وسهلة الحصول عليها مجاناً من خلال مواقع الإنترنت أو آلات البحث ، وذلك للبحث عن المنافذ المفتوحة ( Port ) في جهاز الكمبيوتر الخاص بنا . وعندما يجد الهاكرز المنافذ المفتوح يستخدم البرنامج الخاص بذلك المنافذ ، وهناك طرق تستخدم من قبل كبار الهاكرز للإختراق دون الحاجة لبرامج الإختراق ودون الحاجة لمعرفة المنافذ ( Port ) فإما عن طريق معرفة رقم الـ IP أو بطرق الإرسال العشوائي ، وبالنسبة للهاكرز إن برامج الحماية من خطر الإنترنت تعتمد على بصمة الملفات فقط وأي هاكر يستطيع تغيير بصمة برنامجيه بحيث لا تتعرف برامج الحماية على تلك الملفات وذلك من خلال برامج الهاكرز المختصة بتغيير بصمة البرامج .

والدليل إن الكثير من الأجهزة و الشبكات العالمية والبنوك تم إختراقها ولو كانت هذه البرامج ذات فعالية لتمكنت من حماية البنوك والشبكات والجامعات المختلفة وشركة الاتصالات .

## إذا ما هو الحال

نعتبر أن هؤلاء الهاكرز والكراركرز الذين يضرون أجهزتنا ويخترقون مواقعنا ويسرقون نقودنا هم بالفعل أناس لا ضمير ولا أخلاق لهم ، لذلك لا بد من أخذ الحيطة لحماية سرية المعلومات الخاصة بأجهزتنا ومواقعنا وشبكاتنا و برامج التداول المالية عبر الإنترنت بما فيها الأسهم والبورصات والتعاملات المالية كالحسابات البنكية وبطاقات الائتمان وغيرها .

لذلك يجب استخدام برامج لحماية الأجهزة وحماية المواقع وحماية الشبكات كبرامج درع الفيروسات **System Virus Armor** للتخلص منها أو عدم دخولها وذلك طبقاً للتقنية العلمية المستخدمة للحماية .

والفصل القادم يقدم لنا أهم برامج الحماية التي يجب الإستعانة بها (بعضها طبعاً وليس كلها) .

## الفصل العاشر

### برامج الحماية

أولاً : برامج حماية الأجهزة :

يمكنك تحديث هذه البرامج وتركيبها بجهازك مجاناً

• برنامج الحماية 8 BitDefender

• تحديث لبرنامج PC-Cillin

• برنامج الحماية 8 McAfee

• برنامج الحماية Panda

• برنامج Ad-Aware SE

• برنامج eTrust EZ Anti-Virus

• برنامج The Cleaner

• برنامج Kaspersky Anti-Virus

• تحديث برنامج Norton AntiVirus

• برنامج Trojan Remover

• برنامج F-Prot Antivirus

• برنامج AVG Anti-Virus 7

وأيضاً يوجد كم هائل من برامج الجدران النارية  
**Firewall** التي تؤمن وتحمي جهازك من التلصص والتجسس  
 والسرقة (الكرakers) ومن المتطفلين (الهاكرز) مثال :

- برنامج **R-Firewall 1**
- برنامج **Outpost Firewall pro 4**
- برنامج **Ashampoo Firewall 1**
- برنامج **BlackICE PC protection 3.6**
- برنامج **Comodo personal Firewall 2.3.5.62**
- برنامج **Core Force**
- برنامج **Hackaer Smacker 2**
- برنامج **Look'n stop 2.05**
- وأخيراً برنامج
- McAfee Personal Firewall plus v.5.0.1.5**

ثانياً : برامج لإدارة كلمات السر

هناك أيضاً برامج كثيرة يمكنك تحميلها أو تحديثها من مواقع الإنترنت  
 المختلفة ، مثال هذه البرامج :

١ . برنامج **PassWord manager**

برنامج يدير كلمات السر في جهازك وتخزينها

## ٢. برنامج 1<sup>st</sup> screen lock

يمكنك هذا البرنامج لعمل كلمات سر لحماية جهازك وشبكة الإنترنت.

## ٣. برنامج Hidesfiles 1.1

بهذا البرنامج يمكنك أن تخفي ملفاتك بطريقة آمنة ، وهذه الطريقة لا يمكن لأحد أن يسرق معلوماتك .

## ٤. برنامج Excel pass word recovery 1

برنامج لكسر تشفير ملفات الإكسيل

## ٥. برنامج Outlook password v.9

إستعادة كلمة السر في برنامج out look عند فقدانها

## ٦. برنامج IE internet security

برنامج لحماية كلمات السر المستخدمة في المتصفح browser

## ٧. برنامج KeyPass 4.2.2

برنامج يدون لك كلمات المرور الخاص بك ويحفظها ويديرها مهما كانت كثيرها .

## ٨. برنامج Face Code v2.1.4

من أهم برامج حماية جهازك ومعلوماته حيث أنه بهذا البرنامج



يمكنك تخزين صورتك به ليكون وجهك هي كلمة السر للدخول لجهازك وذلك طبعاً يستلزم وجود كاميرا.

## ٩. برنامج safe input 1.2

إن كنت ممن تقوم بعملية الشراء والبيع عبر شبكة الإنترنت فهذا البرنامج هام جداً لك ، حيث أنه يكشف ملفات التجسس التي تدخل إلى جهازك أثناء كتابتك لكلمات السر.

## ١٠. وأخيراً برنامج Windows Guard

الذي يمكنكم من حماية كلمة السر الخاصة ببرامجك وويندوز.

## ثالثاً : برامج لمكافحة التجسس

### ١. برنامج A2freesetup

هذا البرنامج له قدرة على الإستكشاف وله القدرة على إزالة

### التروجان Trojan

### ٢. برنامج Advanced spyware remover

لمكافحة ملفات التجسس

### ٣. برنامج Anti Trojan Elite

أسرع برنامج في البحث عن ملفات التجسس وأحصنة طروادة

Trojan والديدان worms وهذا البرنامج يجمع بين

الحماية والتسريع والتصلح ..

#### ٤. برنامج Defense wall 1.65

وهو برنامج دفاعي يقاوم ملفات التجسس spy ware

والتروجان Trojan

#### ٥. برنامج Anti worm

لكشف وحذف ملفات التجسس مثل Trojan و worms

### رابعاً : برامج تشفير الملفات

#### ١. برنامج Dekart private desk

يجعل الملفات غير مرئية باستخدام عملية تشفير محمية

#### ٢. برنامج File Buddy

يسمح هذا البرنامج بتشفير الملفات ثم فكها بسهولة

#### ٣. برنامج easy file and folder protector

يقوم بتشفير الملفات وإخفائها بشكل آمن .

#### ٤. برنامج Folder lock

أيضاً يقوم بإخفاء الملفات برقم سري وحمايتها من المتطفلين.

#### ٥. برنامج Masker 7

يقوم أيضاً بعملية تشفير الملفات وإخفائها بكلمة سر

## كيفية الحصول على برامج الحماية مجاناً :

يمكنك الذهاب إلى مواقع التحديث المجاني أو مواقع المنتديات التي تقدم هذه التحديثات المجانية ويتم عمل هذا إتبع الخطوات الآتية :

١. قم بالدخول إلى آلات بحث تدعم اللغة العربية مثال

• [www.google.com.eg](http://www.google.com.eg) جوجل

• أو موقع أرابو [www.arabo.com](http://www.arabo.com)

• أو موقع أرابي [www.araby.com](http://www.araby.com)

٢. أكتب في خانة البحث باللغة العربية : " برامج الحماية "

٣. سيظهر لك مئات المواقع والمنتديات المصاحبة لها تقدم خدمة

تحديث برامج الحماية مجاناً ومثال لهذه المواقع :

• [www.books4internet.com](http://www.books4internet.com)

• [www.absba.com](http://www.absba.com)

• [www.arabsgate.com](http://www.arabsgate.com)

• [www.sultan.org](http://www.sultan.org)

• ومواقع كثيرة أخرى قم بإكتشافها بنفسك

٤. حينما تجد نفسك داخل إحدى هذه المواقع ستبدأ البحث

وغالباً ما ستجد الموضوع الذى تبحث عنه فى أول نافذة كما هو الحال إذا كان الموضوع الذى تبحث عنه داخل مواضيع المنتدى الخاص بالموقع ..

٥. معظم أصحاب المنتديات يطلبون منك أن تسجل بالمنتدى قبل الدخول لرؤية الموضوع ، قم بالتسجيل بلا خوف . فقد أصبحت المنتديات هذه الآونه من أهم الأماكن داخل شبكة الإنترنت التى منها يمكنك أخذ كم هائل من المعلومات والبرامج مجاناً.

## الفصل الحادي عشر

### أهمية المتكامله لجهازك :

اولاً : تحتاج هذه البرامج ان تكون بجهازك :

#### Norton AntiVirus 2002 -1

برنامج حمايه غني عن التعريف

#### 2- برنامج The Cleaner

برنامج حمايه من جميع السيرفرات المسربة للمعلومات - ويفضل ترقية كل فترة لتحديثه للقضاء على التروجانات والفيروسات

#### 3- WinPatrol 3.2

لمسح ملفات الكوكيز التي تضعها بعض المواقع في الاكسلورر

#### 4- برنامج Ad-aware v5.6

لمسح ملفات الكوكيز الموجوده ضمن الملفات والبرامج في جهازك

#### 5- برنامج ZoneAlarm Pro

للحماية من الهاكرز

من إحتوى جهازه على هذه البرامج أعتقد أنه سيتمتع بحماية جيده ولكن

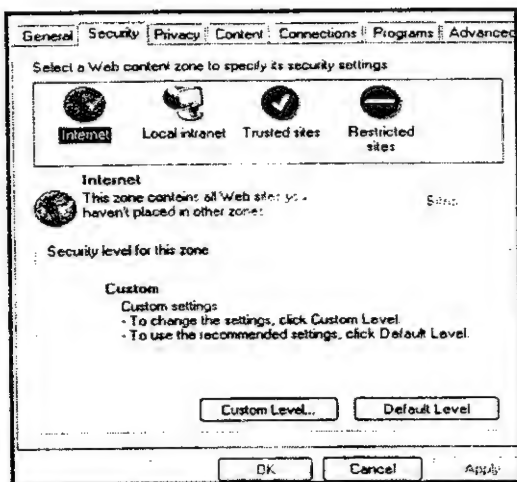
يجب القيام بتحديث البرنامج (١ و ٢ و ٥) بشكل دائم.  
وطبعاً يمكنك إختيار برامج أخرى مشابهة لهذه البرامج ..

**ثانياً : عدم تحميل المواقع الإباحية من خلال جهازك :**

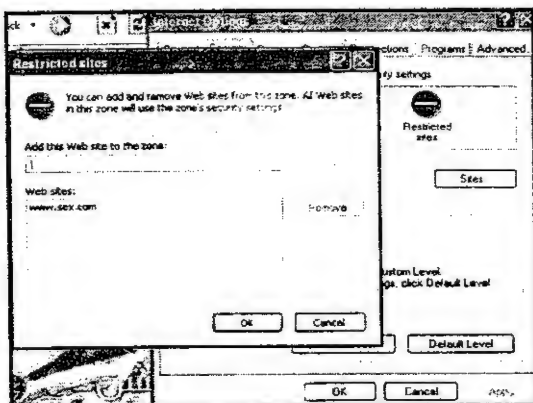
في الحقيقة أن معظم الفيروسات وملفات التجسس يتم غرسها في جهازك من خلال فتح أو تحميل المواقع الإباحية عن طريق جهازك ، لذلك يجب وضع برامج أو طرق لمنع تنزيل هذه المواقع إلى جهازك ، وهناك طرق كثيرة لمنع هذه المواقع فثانياً أن تدخل جهازك :

**الطريقة الأولى : باستخدام اوامر ويندوز**

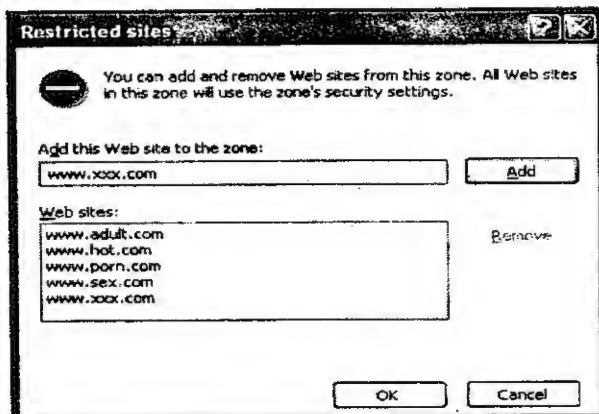
- اذهب إلى Tools من خلال المتصفح إنترنت إكسبلورر
- اختر internet options
- ستحصل على نافذة
- اضغط على security كما يلي:



- قم بالضغط على **Restricted sites**
- قم بالضغط على كلمة **sites** لتحصل على نافذة كما يلي:



• في خانة add this sites to the zone ضع كل المواقع الإباحية التي يشبه بها ثم اضغط OK كما يلي :



### الطريقة الثانية : باستخدام الآت البحث والدلائل

أحياناً ونحن نبحث داخل الشبكة تأتي إلينا إعلانات مخلة أو صور خليعة لكي نتلاشى كل هذا بل ولكي تمنع تماماً المواقع الإباحية من آلات البحث والدلائل ، يمكننا تغيير بعض خصائص آلة البحث لكي تمنع فئات أي موقع إباحي حتى ولو حاولت بنفسك كتابة أي كلمة إباحية فلن يظهر أبداً هذا الموقع وهذا طبعاً يقينا وبقي أبنائنا من تلصص الأعداء الذين يريدون كسر عزائم أمتنا العربية وتسمى هذه العملية بعملية الفلترة **Filtration** ومعظم آلات البحث و الدلائل تملك



ضمن خصائصها هذه العملية التي ترشح أى موقع إباحى وعدم دخوله داخل متصفحاتنا .

و قد وفقنى الله سبحانه وتعالى فى جمع بعض هذه الآلات وكيفية تغيير وظائفها وخصائصها لتكون آمنين ونحن نعمل داخل الشبكة ومنها .

## 1- Yahoo: Set the Safe Search Filter option via page. Search Preferences the

بالدخول إلى موقع ياهو - قم بتسجيل الدخول - قم بالذهاب إلى preferences وفى خانة safesearch قم بالضغط على كلمة edit وحول كلمة off إلى كلمة on

إذهب إلى search ثم قم بالبحث عن أى كلمة إباحية أو حتى موقع إباحى لم تجد له أثر ، الآن أنت وأبنائك فى آمان .

2- Google: See the SafeSearch help page for instructions on setting up filtering on a permanent or as-needed basis.

بنفس طريقة ياهو قم بتغير الخصائص

3- AOL Search: Doesn't appear to offer a filter, but enabling Parental Controls might have an impact on web search matches.

4- Ask Jeeves: Use options for Content Filtering on the Your Settings page or try Ask Jeeves For Kids, listed above.

5- AltaVista: Use the Family Filter Setup page.

بنفس الطريقة اذهب إلى هذه الخاصية وقم بتغييرها

6- HotBot: Use the Block Offensive Content section of the Filter Preferences page. Note that you may need to set this again if you change from using the default "HotBot" search engine that's offered.

7- LookSmart: LookSmart has never accepted

adult content for listing within its directory results. However, obscure queries might bring these up in the crawler-based results that are sometimes provided.

8- Lycos: Use the Adult Filter section of the Advanced Search Filters page.

9- MSN Search: Use the Safe Search Filter on the Settings page.

10 - AllTheWeb: Use the Basic Settings page to enable the Offensive Content Filter option. The only works for searches in English.

## الطريقة الثالثة : برامج منع المواقع الإباحية Filtering and Blocking Software

أما هذه الطريقة فهي برامج تعمل من داخل الويب نفسه وليس فقط نتائج البحث .

وهناك برامج كثيرة تقوم بهذه المهمة ومن ضمن هذه البرامج ما يلي :

## **1- Cyber Patrol**

**<http://www.cyberpatrol.com/>**

**The program can filter web pages, newsgroups, chat rooms and other internet resources, and can be used to limit online time, create user logs and so on.**

## **2- Net Nanny**

**<http://www.netnanny.com/>**

**Looksmart acquired Net Nanny in April 2004 and added porn-free web search to the product shortly thereafter. The product provides a wide variety of parental controls, including blocking content based on content, URL, or ratings. In addition to blocking web pages, the program allows selective blocking of access to chat, instant messaging, internet games and newsgroups. The program can also be configured to prevent illegal downloading of copyrighted or obscene material.**

### 3- Web Blocker

[www.web-blocker.com](http://www.web-blocker.com)

برنامج جميل جداً لعدم فتح المواقع الإباحية  
وإليك الشرح بالتفصيل :

قم بتزيل وتثبيت برنامج

**weblocker**

<http://www.web-blocker.com>

من هذا الرابط . هذا البرنامج يقوم بمنع الدخول على المواقع الإباحية  
فهاثيا . وهو برنامج رائع حقاً وخفيف ولا يقوم بالتأثير فهاثيا على سرعة  
الإتصال . ويحتاج هذا البرنامج بعد تنزيله أن تكتب له كلمة سر .  
وسؤال سري .

#### **Password and secret question**

لأنه من غير أحدهما لا يستطيع أحد أن يزيل البرنامج من على الجهاز  
المثبت عليه . وإذا حدث وحاول أحد أن يمسح ملفات البرنامج فإن  
البرنامج يمنع الدخول على الشبكة فهاثيا ، إلى أن يقوم بإعادة تثبيت  
البرنامج من جديد . لكن يتبادر سؤال ، طالما أنا الذى سأضع كلمة  
السر هذه فرما راودنى الشيطان ونفسى الأمانة بالسوء إلى إزالة  
البرنامج فى أى وقت ومعاودة المعصية مرة أخرى ؟ نقول بأنك لابد أن

تضع كلمة سر بحيث تنساها أنت نفسك ، وهذا بطريقة سهلة جداً

١ افتح ملف وورد أو أى برنامج كتابة

٢ أغمض عينيك وأضغط على لوحة المفاتيح عشوائياً لمدة دقيقة مثلاً .

سينتج عن ذلك سطر طويل من الحروف الإنجليزية العشوائية .

٣ اختر بالفأرة من وسط هذا السطر أى جزء عشوائياً " تقريباً ١٥

حرف مثلاً أو أقل أو أكثر قليلاً

٤ قم بنسخ هذا الجزء ، ثم هناك فى البرنامج فى الجزء المخصص

لإدخال كلمة السر ( يطلب البرنامج إدخالها فى مكانين ) ألصق ما

نسخته

أنقر بالزر الأيمن للفأرة على المكان المخصص وأختر

paste أو أضغط **ctrl+v**

وفى مكان إدخال السؤال السرى أكتب أى شىء ، وفى مكان إجابة

السؤال السرى يمكن أن تنسخ وتلصق جزء آخر من السطر الذى

كتبته .

٥ أمسح السطر العشوائى الذى كتبته .

وهذا تكون المهمة قد تمت بنجاح الحمد لله وأغلقت عن نفسك باب

واسع للشيطان.

## References

### English refernces

- Ross J. Anderson: *Security Engineering: A Guide to Building Dependable Distributed Systems*, ISBN 0-471-38922-6
- Bruce Schneier: *Secrets & Lies: Digital Security in a Networked World*, ISBN 0-471-25311-1
- Robert C. Seacord: *Secure Coding in C and C++*. Addison Wesley, September, 2005. ISBN 0-321-33572-4
- Paul A. Karger, Roger R. Schell: *Thirty Years Later: Lessons from the Multics Security Evaluation*, IBM white paper.
- Clifford Stoll: *Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Pocket Books, ISBN 0-7434-1146-3
- Stephen Haag, Maeve Cummings, Donald McCubbrey, Alain Pinsonneault, Richard Donovan: *Management Information Systems for the information age*, ISBN 0-07-091120-7
- Peter G. Neumann: *Principled Assuredly Trustworthy Composable Architectures 2004*
- E. Stewart Lee: *Essays about Computer Security* Cambridge, 1999

### Internet websites

### Search engines

### Arabic books

### Magazines

## إصدارات المراكز العلمية لتبسيط العلوم

| م  | إسم الكتاب  | جنيه |
|----|---|------|
| ١  | موسوعة التجارة الإلكترونية (١) البيع والشراء عبر مواقع المزايدات    | ج ١٥ |
| ٢  | موسوعة التجارة الإلكترونية (٢) كيف تصمم موقع ناجح                   | ج ١٢ |
| ٣  | موسوعة التجارة الإلكترونية (٣) التصدير والإستيراد                   | ج ١٢ |
| ٤  | موسوعة التجارة الإلكترونية (٤) التسويق باستخدام البريد الإلكتروني   | ج ١٢ |
| ٥  | موسوعة التجارة الإلكترونية (٥) كيف تبيع المنتجات العربية والإسلامية | ج ١٠ |
| ٦  | موسوعة التجارة الإلكترونية (٦) عملية الـ <b>Drop shipping</b>       | ج ١٠ |
| ٧  | موسوعة التجارة الإلكترونية (٧) التسويق باستخدام الآت البحث          | ج ٨  |
| ٨  | موسوعة التجارة الإلكترونية (٨) البرامج المشاركة                     | ج ٩  |
| ٩  | موسوعة التجارة الإلكترونية (٩) طرق الدفع عبر الإنترنت               | ج ١٠ |
| ١٠ | موسوعة التجارة الإلكترونية (١٠) تعلم اللغة الإنجليزية التجارية      | ج ١٢ |
| ١١ | موسوعة التجارة الإلكترونية (١١) خدمة العملاء عبر الإنترنت           | ج ١٠ |
| ١٢ | موسوعة التجارة الإلكترونية (١٢) أمن المعلومات                       | ج ١٠ |
| ١٣ | موسوعة التجارة الإلكترونية مشروع (١) كيف تبيع e-book                | ج ٥  |
| ١٤ | موسوعة التجارة الإلكترونية مشروع (٢) التعليم عن بعد                 | ج ٥  |
| ١٥ | موسوعة التجارة الإلكترونية مشروع (٣) عمل أرباح بواسطة Google        | ج ٥  |
| ١٦ | موسوعة التجارة الإلكترونية مشروع (٤) Pay per click PPC              | ج ٥  |
| ١٧ | موسوعة التجارة الإلكترونية مشروع (٥) Pay per register               | ج ٥  |
| ١٨ | موسوعة التجارة الإلكترونية مشروع (٦) بيع الكتب عبر الإنترنت         | ج ٥  |
| ١٩ | موسوعة التجارة الإلكترونية مشروع (٧) بيع منتجات الغير عبر موقعك     | ج ٥  |
| ٢٠ | موسوعة التجارة الإلكترونية مشروع (٨) إستيراد المنتجات بأقل الأسعار  | ج ٥  |



|      |    |   |
|------|----|---|
| ج ٥  | ٢١ | موسوعة التجارة الإلكترونية مشروع (٩) تصدير المنتجات العربية     |
| ج ٥  | ٢٢ | موسوعة التجارة الإلكترونية مشروع (١٠) كيف تسوق موقعك            |
| ج ١٠ | ٢٣ | Jobs online وكتابة السيرة الذاتية                               |
| ج ١٠ | ٢٤ | البحث داخل شبكة الإنترنت  |
| ج ١٠ | ٢٥ | دليل المواقع التجارية   |
| ج ١٠ | ٢٦ | دليل المواقع الصحية   |
| ج ١٤ | ٢٧ | دليل المواقع العلمية  |
| ج ١٠ | ٢٨ | 2006 online sellers   |
| ج ٩  | ٢٩ | كيف تصبح مبدعاً (جديد ١٠٠%)                                     |
| ج ٩  | ٣٠ | كيف تصبح مسوقاً ناجحاً (جديد ١٠٠%)                              |
| ج ٩  | ٣١ | كيف تصبح خبيراً في صيانة الموبايل (جديد ١٠٠%)                   |
| ج ٩  | ٣٢ | كيف تصبح خبيراً في الأسهم والبورصة (جديد ١٠٠%)                  |
| ج ٥  | ٣٣ | سلسلة مقارنات (١) عمرو و عمرو                                   |
| ج ٥  | ٣٤ | سلسلة مقارنات (٢) أكاديمي و أكاديمي (وأعداد كثيرة أخرى)         |
| ج ٥  | ٣٥ | Html والويب   |
| ج ٥  | ٣٦ | Front page والويب   |
| ج ٥  | ٣٧ | مايكروسوفت أوفيس والويب   |
| ج ٥  | ٣٨ | فوتوشوب والويب  |
| ج ٧  | ٣٩ | موسوعة أسرار الكمبيوتر والإنترنت رقم ١ مقدمة في الحاسب الآلى    |
| ج ١٢ | ٤٠ | موسوعة أسرار الكمبيوتر والإنترنت رقم ٢ ويندوز windows           |
| ج ١٠ | ٤١ | موسوعة أسرار الكمبيوتر والإنترنت رقم ٣ معالجة الكلمات وورد Word |
| ج ١٠ | ٤٢ | موسوعة أسرار الكمبيوتر والإنترنت رقم ٤ إكسيل Excel              |
| ج ١٠ | ٤٣ | موسوعة أسرار الكمبيوتر والإنترنت رقم ٥ باور بوينت power point   |
| ج ١٠ | ٤٤ | موسوعة أسرار الكمبيوتر والإنترنت رقم ٦ أكسيس Access             |

|    |  |      |
|----|--|------|
| ٤٥ | موسوعة أسرار الكمبيوتر والإنترنت رقم (٧) إنترنت إكسبلورر         | ج ٧  |
| ٤٦ | الإنترنت و أولادك  | ج ٧  |
| ٤٧ | ثورة الإنترنت  | ج ٧  |
| ٤٨ | دليل المواقع على الإنترنت  | ج ٧  |
| ٤٩ | تعلم اللغة الإنجليزية من البداية إلى الإحتراف                    | ج ١٢ |
| ٥٠ | كن مسلماً عبر شبكة الإنترنت                                      | ج ٥  |
| ٥١ | كن داعياً عبر شبكة الإنترنت                                      | ج ٥  |
| ٥٢ | كيف تستخدم الإنترنت لتقول للعالم من هو محمد (صلى الله عليه وسلم) | ج ٥  |
| ٥٣ | وافلسطين   | ج ٣  |
| ٥٤ | العلم الحديث وأثره في الدعوة الإسلامية                           | ج ٥  |
| ٥٥ | موسوعة أمراض العظام والكسور والعمود الفقري                       | ج    |
| ٥٦ | صيدلية في كل منزل  | ج ٥  |
| ٥٧ | شنترة سفر  | ج ٥  |
| ٥٨ | رحلة إلى الصين   | ج ٥  |
| ٥٩ | كومبو والشاطرنت  | ج ٥  |
| ٦٠ | موسوعة كيف تشتري ؟   | ج ٥  |

برجاء زيارة موقعنا للحصول على العروض والخصومات الخاصة

[www.books4internet.com](http://www.books4internet.com)

## دورات التجارة الإلكترونية - البيع والشراء عبر شبكة الإنترنت

### ١ - دورة التاهيل للعمل بالتجارة الإلكترونية

#### • Word XP ورود

• طريقة البحث داخل الشبكة و عمل بريد إلكتروني وماسنجر

• اللغة الإنجليزية التجارية للعمل بها عبر الإنترنت

i. كيفية كتابة رسالة بريد إلكتروني e-mail باللغة الإنجليزية

ii. كيفية كتابة محتوى موقع website باللغة الإنجليزية

iii. مصطلحات التجارة الإلكترونية والإستيراد والتصدير

iv. مشروع التخرج

### ٢- دورات التجارة الإلكترونية

#### ١- المستوى الأول

• ما هي التجارة الإلكترونية وما هي أنواعها وفوائدها

• البيع عبر مواقع المزادات والمخازن الإلكترونية

• وسائل الدفع المختلفة وأهمها الدفع أون لاين payment online

#### ٢- المستوى الثاني

• تصميم موقع برنامج فرونت بيج ثم نشره داخل الشبكة

• عمل برامج مشاركة Affiliate programs والربح الوفير من خلال

هذه البرامج

• الحصول على إعلانات ووضعها بموقعك لعمل أرباح كثيرة

• كيفية الحصول على منتجات لبيعها بموقعك

• كيف تسوق موقعك لجذب الزبائن وجلب زوار كثيرة لموقعك

#### ٣- المستوى الثالث

• الإستيراد والتصدير باستخدام شبكة الإنترنت

• كيفية إنشاء شركة إستيراد وتصدير

- إجراءات التصدير والإستيراد والمستندات اللازمة (الشركة-البنك-الجمارك)
- طرق الشحن ووسائل الدفع والتخليص الجمركي
- طرق الحصول على منتجات وأهم المواقع المستخدمة للتصدير والإستيراد

## ٤- المستوى الرابع

- إستراتيجيات التسويق
- التسويق بواسطة البريد الإلكتروني
- التسويق بواسطة آلات البحث والدلائل
- التسويق بواسطة مواقع إنترنت خاصة بالتجارة الدولية
- التسويق بواسطة المنتديات والقوائم البريدية وبرامج الشات messenger و الرسائل القصيرة عبر الإنترنت sms

## ٣- دورات مكمل للـ التجارة الإلكترونية

١. فوتوشوب Photoshop :
- كيفية تصميم بانر banner ولوجو وصور المنتجات برنامج فوتوشوب
- كيفية تصميم موقع بواسطة برنامج فوتوشوب Photoshop
٢. كيفية تصميم موقع بواسطة برنامج باور بونت power point
٣. كيفية تركيب منتدى Forum بموقعك وإدارة عمله بواسطة control panel
- كيفية عمل القوائم البريدية mailing list

للسؤال عن اسعار هذه الدورات وأكجز برجاء مراسلتنا

E-mail: scss2004@yahoo.com

scss@books4internet.com

## تنبيه هام:

قبل أن تشتري أى كتاب من كتب موسوعة التجارة الإلكترونية تأكد من أن المؤلف هو خالد محمد خالد وذلك لأنه للأسف لوحظ في الآونة الأخيرة أن أحد دور النشر المعروفة قد سرقت أبواب كاملة من الموسوعة ووضعتها في كتاب تحت إسم التجارة الإلكترونية ويتم بيعها الآن بالأسواق. وللأسف هذا الكتاب تم نقله بإسلوب غير مفهوم وغير منسق لأنه تم إعداده بمعرفة شخص ليس له علاقة بالتجارة الإلكترونية سوى جنى المال فقط.

## المحتويات

|    |  |
|----|--|
| ٦  | مُعِيد                                   |
|    | المقدمة                                  |
| ٧  | حينما أصبحت ضحية الهاكرز كتبت هذه الكتاب |
|    | الفصل الأول                              |
| ١٧ | مصطلحات أمن المعلومات والمواقع والحاسبات |
|    | الفصل الثاني                             |
| ٣٩ | أمن المعلومات                            |
|    | الفصل الثالث                             |
| ٤٧ | الهاكرز والكرakers                       |
|    | الفصل الرابع                             |
| ٥١ | أنواع الهجوم والإختراق                   |

## الفصل الخامس

٥٥ التخلص من الفيروسات وملفات التجسس

## الفصل السادس

٦٩ الحفاظ على البريد الإلكتروني من الإختراق

## الفصل السابع

٧٣ تأمين الدفع الإلكتروني

٧٥ بروتوكول S-HTTP

٧٧ SSL بروتوكول

٨٢ بروتوكول الحركات المالية الآمنة SET

٨٤ عملية الشراء وفقاً لبروتوكول الحركات المالية الآمنة (SET)

٨٦ إجراء الحركات المالية وفقاً لبروتوكول الحركات المالية الآمنة SET

## الفصل الثامن

٨٩ طرق أمن المعلومات والحفاظ على البيانات

## الفصل التاسع

٩٥ الثغرات

## الفصل العاشر

برامج الحماية

١٠١

## الفصل الحادي عشر

الحماية المتكاملة لجهازك

١٠٨

أولاً: البرامج التي يجب أن تكون بجهازك

١٠٨

ثانياً : عدم تحميل المواقع الإباحية من خلال جهازك

١٠٩

## المراجع

١١٨

إصدارات المركز

١١٩

دورات تدريبية

١٢٢

تنبيه

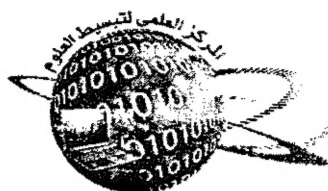
١٢٤

## المحتويات

١٢٥



## الناشر



المركز العلمي لتبسيط العلوم

٢٣ من رفعت، سيدى بشر، إسكندرية

تليفون: ٥٢٩٨٤٢٨ - فاكس: ٥٢٩٨٤٢٨

International: 0106367467

[www.books4internet.com](http://www.books4internet.com)

[scss@books4internet.com](mailto:scss@books4internet.com)